

Table 13.1 Available Recovery Console Commands (continued)

Command	Explanation
fixboot	<p>Writes a new boot sector onto the system partition.</p> <p><code>fixboot [drive:]</code></p> <p><code>drive:</code> Specifies the drive to which a boot sector will be written, overriding the default choice of the system boot partition.</p>
fixmbr	<p>Repairs the master boot code of the boot partition.</p> <p><code>fixmbr [device-name]</code></p> <p><code>device-name</code> Optional name that specifies the device that needs a new MBR. If this is left blank then the boot device is used.</p> <p>If fixmbr detects an invalid or nonstandard partition table signature, it prompts you before rewriting the MBR.</p> <p>Warning</p> <p>This command can damage your partition table if a virus is present or a hardware problem exists and causes partitions to become inaccessible. It is recommended that you run antivirus software before using this command.</p> <p>Windows 2000 includes the antivirus software AvBoot. For more information about AvBoot, see “Troubleshooting Strategies” in this book.</p>
format	<p>Formats a disk for use with Windows 2000.</p> <p><code>format [drive:] [/q] [/fs:file-system]</code></p> <p><code>[drive:]</code> Specifies the drive to format.</p> <p><code>/q</code> Performs a quick format.</p> <p><code>/fs:file-system</code> Specifies the file system to use (FAT, FAT32, or NTFS)</p>
help	<p>Displays information about commands supported by the Recovery Console.</p> <p><code>help [command]</code></p> <p><code>command</code> Any Recovery Console command.</p> <p>If <code>command</code> is not specified, all of the commands supported by the Recovery Console are listed. The <code>command</code> parameter is used to see the help for a specific command.</p>
listsvc	<p>Lists all available services and drivers on the computer.</p>
logon	<p>Lists the detected installations of Windows 2000, and requests the local administrator password for those installations.</p>

continued

Table 13.1 Available Recovery Console Commands (*continued*)

Command	Explanation
map	Lists the drive letter to physical device mappings that are currently active. map [arc]
	arc Tells MAP to use ARC paths instead of Windows 2000 device paths.
md/mkdir	Creates a directory. md [drive:]path mkdir [drive:]path
	Mkdir only operates within the system directories of the current Windows installation, removable media, the root directory of any hard disk partition, or the local installation sources.
more/type	Displays a text file to the screen. more [filename] type [filename]
	More or type displays a text file.
rd/rmdir	Removes (deletes) a directory. rd [drive:]path rmdir [drive:]path
	Rmdir only operates within the system directories of the current Windows installation, removable media, the root directory of any hard disk partition, or the local installation sources.
ren/rename	Renames a single file. ren [drive:][path]filename1 filename2 rename [drive:][path]filename1 filename2
	You cannot specify a new drive or path for your destination file.
	Rename only operates within the system directories of the current Windows installation, removable media, the root directory of any hard disk partition, or the local installation sources.

continued

Table 13.1 Available Recovery Console Commands (continued)

Command	Explanation								
set	<p>Displays and sets Recovery Console environment variables.</p> <pre>set variable = parameter</pre> <pre>set AllowWildCards = TRUE</pre> <p>The following environment variables are supported:</p> <table><tr><td>AllowWildCards</td><td>Enable wildcard support for some commands, such as DEL, that do not otherwise support them.</td></tr><tr><td>AllowAllPaths</td><td>Allow access to all files and folders on the computer.</td></tr><tr><td>AllowRemovableMedia</td><td>Allow files to be copied to removable media, such as floppy disks.</td></tr><tr><td>NoCopyPrompt</td><td>Do not prompt when overwriting file.</td></tr></table> <p>To display the list of current environment variable settings, type set without parameters.</p> <p>The set command is an optional Recovery Console command that can be enabled by using either the Group Policy snap-in or the Security Configuration and Analysis snap-in.</p>	AllowWildCards	Enable wildcard support for some commands, such as DEL, that do not otherwise support them.	AllowAllPaths	Allow access to all files and folders on the computer.	AllowRemovableMedia	Allow files to be copied to removable media, such as floppy disks.	NoCopyPrompt	Do not prompt when overwriting file.
AllowWildCards	Enable wildcard support for some commands, such as DEL, that do not otherwise support them.								
AllowAllPaths	Allow access to all files and folders on the computer.								
AllowRemovableMedia	Allow files to be copied to removable media, such as floppy disks.								
NoCopyPrompt	Do not prompt when overwriting file.								
systemroot	Sets the current directory to %SystemRoot%.								

Often it is useful to enable the **set** command to make full use of the Recovery Console. To do this, a local policy must be enabled.

► **To enable full functionality of the set command using Group Policy**

Note If Group Policy has already been added to your MMC, skip to step 8.

1. From the **Start**, click **Run**, and then type
mmc
2. Press **ENTER**.
3. In the **Console1** dialog box, click **Console**, select **Add/Remove Snap-in**, and then click **Add**.
4. Select **Group Policy**, and then click **Add**.
5. In the **Select Group Policy Object** list box, choose **Local Computer**, and then click **Finish**.
6. In the **Add Standalone Snap-in** dialog box, click **Close**.
7. In the **Add/Remove Snap-in** dialog box, click **OK**.
8. Expand **Local Computer Policy**, **Computer Configuration**, **Windows Settings**, **Security Settings**, and then **Local Policies**. Click **Security Options**.

9. Double-click the policy **Recovery Console: Allow floppy copy and access to all drives and folders**.
10. In the **Local Security Policy Setting** dialog box, select **Enabled**, and then click **OK**.

► **To enable full functionality of the set command using the Security Configuration and Analysis snap-in**

Note If Security Configuration and Analysis snap-in has already been added to your MMC, skip to step 7.

1. From the **Start**, click **Run**, and then type
mmc
2. Press **ENTER**.
3. In the **Console1** dialog box, click **Console**, select **Add/Remove Snap-in**, and then click **Add**
4. Select **Security Configuration and Analysis**, click **Add**, and then click **Close**. In the **Add/Remove Snap-in** dialog box, click **OK**.
5. In the **Console1** dialog box, double click **Security Configuration and Analysis**. Follow the instruction to either open an existing database or create a new database.
6. In the **Console1** dialog box, follow the instructions to configure your computer and analyze your computer security settings.
7. In the **Security Configuration and Analysis** snap-in, double click **Security Configuration and Analysis**.
8. Expand **Local Policies**, and then click **Security Options**.
9. Double-click the policy **Recovery Console: Allow floppy copy and access to all drives and folders**.
10. In the **Analyzed Security Policy Setting** dialog box, select **Enabled**, and then click **OK**.

Note You can also use the Group Policy snap-in and the Security Configuration and Analysis snap-in to select the policy **Recovery Console: Allow automatic administrative logon**.

Replacing the Registry Using the Recovery Console

If you are having problems with the registry, you can use the **copy** command to replace individual registry files by copying them from either the %SystemRoot%\Repair folder or the %SystemRoot%\Repair\RegBack folder.

Important If you copied the files from %SystemRoot%\Repair\RegBack, your registry settings reflect those that were in effect when you selected the **System State** option during Backup operations.

If you copied the files from %SystemRoot%\Repair, your registry settings reflect those that were in effect when you installed Windows 2000.

Recreating Boot.ini Using the Recovery Console

You can use the Emergency Repair Process to replace a missing or corrupted Boot.ini file. Alternatively, you can use the **map** command to determine the location of the disks. With this information, you can create a Boot.ini file on another computer, and then use a floppy disk to transfer the Boot.ini file to the original computer.

Using the Emergency Repair Disk

If your system does not start, and using safe mode or the Recovery Console has not helped, you can try using the Emergency Repair Disk (ERD) option of Backup. Backup includes a wizard to help you create an ERD. If a system failure occurs, you can start the system using the Windows 2000 Setup CD or the Windows 2000 Setup floppy disks which can be created by running Makeboot.exe from the Bootdisk folder on the Windows 2000 Setup CD. Then use the Emergency Repair Process to restore core system files.

Make sure to create an ERD when your computer is functioning well so that you are prepared if you need to repair system files. The ERD allows you to make only basic system repairs, such as to the system files, boot sector, and startup environment. The ERD does not back up data, programs, or the registry and is not a replacement for regular system backups.

Important The Windows 2000 ERD, unlike the ERD used with Windows NT, does not contain a copy of the registry files. The backup registry files are in the folder %SystemRoot%\Repair. However, these files are from the original installation of Windows 2000. In the event of a problem, they can be used to return your computer to a usable state.

When you back up system state data, a copy of your registry files is placed in the folder %SystemRoot%\Repair\Regback. If your registry files become corrupted or are accidentally erased, use the files in this folder to repair your registry without performing a full restore of the system state data. This method is recommended for advanced users only and can also be accomplished by using the Recovery Console commands.

Creating the Emergency Repair Disk

When the ERD is created, the files listed in Table 13.2 are copied from %SystemRoot%\Repair to a floppy disk.

Table 13.2 Contents of the Repair Directory Created by Windows 2000 Setup

File Name	Contents
Autoexec.nt	A copy of %SystemRoot%\System32\Autoexec.nt, which is used to initialize the MS-DOS environment.
Config.nt	A copy of %SystemRoot%\System32\Config.nt, which is used to initialize the MS-DOS environment.
Setup.log	A log of which files were installed files, and Cyclic Redundancy Check (CRC) information for use during the Emergency Repair Process. This file has the read-only, system, and hidden attributes, and it is not visible unless you have configured My Computer to show all files.

Create the ERD after Windows 2000 is installed. Recreate the ERD after each service pack, system date, or updated driver is installed. Be sure to make a copy of your current ERD and store it in a secure location, perhaps off-site.

Note The ERD is not a replacement for backups!

For more information about the %SystemRoot%\Repair and %SystemRoot%\System32\Config folders and the ERD, see the Knowledge Base link on the Web Resources page
<http://windows.microsoft.com/windows2000/reskit/webresources>.

Emergency Recovery Process

If you have prepared an ERD, you can use it to help repair system files after starting the computer using either the Windows 2000 Setup CD or the Windows 2000 Setup floppy disks. However, the Windows 2000 Setup CD is required for replacing any damaged files.

The ERD must include current configuration information. Make sure that you have an ERD for each installation of Windows 2000 on your computer, and never use an ERD from another computer.

Note You cannot repair all disk problems by using the ERD.

When you start the Emergency Repair Process, the following information is displayed on the screen:

This operation will attempt to repair your Windows 2000 system.

Depending on the type of damage present, this operation might or might not be successful. If the system is not successfully repaired, restart Setup and choose the option to recover a destroyed system or system disk.

Select one of the following repair options:

- **Manual Repair.** To choose from a list of repair options, press M.
- **Fast Repair.** To perform all repair options, press F.

If you select **Manual Repair**, the registry files are not checked. If you select **Fast Repair**, and if the folder %SystemRoot%\Repair is accessible, the registry files are checked. If the folder %SystemRoot%\Repair is inaccessible (for example, due to file system corruption) the registry files are not checked.

- **Manual Repair.** It is recommended that only advanced users or administrators choose this option. Using it, you can repair system files, boot sector problems, and startup environment problems.

- **Fast Repair.** This is the easier option to use, and does not require user input. If you choose this option, the Emergency Recovery Process attempts to repair problems related to system files, the boot sector on your system disk, and your startup environment (if your computer has more than one operating system installed). This option also checks and repairs the registry files by loading and unloading each registry key. If a key is not successfully checked, it is automatically copied from the repair directory to the folder %SystemRoot%\System32\Config.

If you choose Fast Repair, all repair options are performed. Manual Repair allows you to select from the following three options:

Inspect Startup Environment Inspect Startup Environment verifies that the Windows 2000 files in the system partition are correct. If any of the files that are needed to start Windows 2000 are missing or corrupted, Repair replaces them from the Windows 2000 Setup CD. These include NTLDR and Ntdetect.com. If Boot.ini is missing, it is recreated.

Verify Windows 2000 System Files Verify Windows 2000 System Files uses a checksum to verify that each installed file is good and that it matches the file that was installed from the Windows 2000 Setup CD. If the recovery process determines that a file on the disk does not match what was installed, it displays a message that identifies the file and asks if you want to replace it. The Emergency Repair Process also verifies that startup files, such as NTLDR and Ntoskrnl.exe, are present and valid.

Inspect Boot Sector Inspect Boot Sector verifies that the boot sector on the system partition still references NTLDR. The Emergency Repair Process can only replace the boot sector for the system partition on the first hard disk. The Emergency Repair Process can also repair the boot sector for the system partition on the startup disk.

If you choose Fast Repair, all repair options are performed.

If the Emergency Repair Process Does Not Fix Your System

If you have performed the Emergency Repair Process and the computer still does not operate normally, you can use the Windows 2000 Setup CD to perform an in-place upgrade over the existing installation. This is a last resort before reinstalling the operating system. Note that the time required to complete the following procedure is equal to the time it takes to reinstall the operating system.

► **To perform an in-place upgrade of Windows 2000**

1. Mount the Windows 2000 Setup CD.
2. Press **Enter** to install a copy of Windows 2000.
3. When you are prompted to repair the existing Windows 2000 installation, press R.

Note Windows 2000 Setup performs an in-place upgrade of your existing installation. However, you might lose some customized settings of your system files.

Restoring System State Data

In Microsoft® Windows® 2000 Server, system state data comprises the registry, COM+ Class Registration database, system startup files, and the Certificate Services database (if the server is a certificate server). If the server is a domain controller, Active Directory™ directory services and the Sysvol directory are also contained in the system state data. If the server is running the Cluster service, the system state data also includes resource registry checkpoints and the quorum resource recovery log, which contains the most recent cluster database information.

When you restore the system state data, all system state data that is relevant to your computer is backed up or restored: you cannot back up or restore individual components of the system state data. This is due to dependencies among the system state components. However, you can restore the system state data to an alternate location, and only the registry files, Sysvol directory files, Cluster database information files, and system startup files are restored to the alternate location. The Active Directory database, Certificate Services database, and COM+ Class Registration database are not restored if you designate an alternate location when you restore the system state data.

Note You can only back up and restore the system state data on a local computer: you cannot back up and restore the system state data on a remote computer.

► **To restore system state data**

1. Start Backup.
2. Click the **Restore** tab, and then select the check box for any drive, folder, or file that you want to restore.

3. Click the box next to **System State** to restore the system state data along with any other data you have selected for the current restore operation.

Caution If you restore the system state data, and you do not designate an alternate location for the restored data, Backup erases the system state data that is currently on your computer and replaces it with the system state data you are restoring.

You must be an administrator or a backup operator to restore files and folders. For more information about restoring the system state data to a domain controller and about authoritative restores, see the *Microsoft® Windows® 2000 Server Resource Kit Distributed Systems Guide*.

Restoring the Registry

When you back up the system state data, a copy of your registry files is also saved in %SystemRoot%\Repair\Regback. If your registry files become corrupted or are accidentally erased, you can use these files to repair the registry without performing a full restore of the system state data. This method is recommended only for advanced users.

Note Backup does not allow you to restore only the registry files. If you use Backup to restore lost data to the registry, all system state data is replaced.

You can also use Backup to restore lost data to the registry. The system must be stable enough for you to open Backup. If your computer cannot start, you might be able to repair the operating system using an ERD. The **Fast Repair** option of the Emergency Repair Process checks and, if necessary, replaces each registry key by copying it from the repair directory to the folder %SystemRoot%\Config.

If you cannot fix the problem with the registry by performing the Emergency Repair Process or by selecting **Last Known Good Configuration** from the **Windows 2000 Advanced Options** menu, it might be necessary to reinstall the operating system and device drivers and to reconfigure the system before you can restore the data.

Restoring Data

If files, the registry, or directory services are not accessible, you need to restore them. Restore operations are only possible if you have used Backup or another program to backup the files on your computer. Backup allows you to restore the entire backup medium, one or more backup sets, or individual files. After the restore operation starts, you have the option of restoring the local registry and directory service as well.

All catalog information is normally maintained on the corresponding medium for that backup set.

When you insert a backup medium to restore information, only information about the first backup set is displayed. To restore the entire medium, load the catalog first. Otherwise, when you select a medium, you are selecting only the displayed sets.

Restoring Files from Third-Party Backup Programs

You can use Backup to restore data from a tape that was backed up with a program other than Backup if the tape is in the Microsoft tape format (MTF). Although the tape might not have the full on-tape catalog (OTC) information that Backup produces, it should have equivalent information. Also, some older tape backup devices might not support creating full OTCs with Backup. Contact the vendor if you suspect that your tape backup device does not support creating a full OTC.

Restoring File Security Settings

Backup preserves permissions, ownership, and audit flags on files restored to NTFS volumes but not on files restored to FAT volumes. It is not possible to secure information on FAT volumes.

When you restore files to a new computer or hard disk, you do not have to restore security information. The files inherit the permissions of the directory in which they are placed. If the directory has no permissions, the file retains its previous permissions, including ownership.

Recovering Your Disk Configuration

In case of a disaster, you can recreate your disk structures and signatures by using the Disk Signature information displayed when you used the Dir command.

You can restore disk, partition, and volume configurations by using the results from the DumpConfig command-line tool (Dumpconfig.exe). For more information about DumpConfig, see the *Distributed Systems Guide*.

Recovering a Mirrored or RAID-5 Volume

The process of error detection and recovery for software fault-tolerant volumes is similar for both mirrored volumes and RAID-5 volumes. The Windows 2000 response to the problem depends on when the problem occurred. For recovery of a hardware fault-tolerant volume, see the documentation for the controller that you are using.

Note Marking a mirror as failed does not occur during a read, only during a write. The read cannot affect the data on the disks, so performing mirror error processing is not necessary.

The operating system usually continues to work normally. Users accessing resources over the network usually are not affected.

Be sure to back up important data immediately, because the volume is no longer fault tolerant. Use a new tape for backup, not an existing tape. Replace the failed disk and begin the recovery of the mirrored volume or RAID-5 volume as soon as possible.

During system initialization, if the system cannot locate a partition in a mirrored volume or a RAID-5 volume, it logs a severe error in the event log, marks the volume as Failed Redundancy and uses the remaining portions of the mirrored volume or RAID-5 volume. The system continues to function by using the fault-tolerant capabilities inherent in such volumes. For more information about the status of volumes displayed in the Disk Management snap-in, see “Planning a Reliable Configuration” in this book.

Recovering a Mirrored Volume

A mirrored volume provides fault tolerance by duplicating data on two disks. If one disk fails, the data on the failed disk becomes unavailable, but the system continues to operate using the unaffected disk.

If the failure of a mirrored volume did not cause any disruption in service, you can continue running in a non-fault-tolerant configuration and schedule a time to reconstruct the mirrored volume. This activity can occur during a normally scheduled maintenance period or during a less busy time. However, if you have a spare disk in the configuration, you can reconstruct the mirror immediately.

Note The failed disk can be replaced with any disk that is the same size or larger. It is a good idea to use a disk as similar to the remaining disk as possible.

When you move or replace a disk that was at the end of a SCSI bus, be sure that you terminate only the disk that is now at the end of the bus.

When a member of a mirrored volume is orphaned, you need to break the mirrored volume to expose the remaining volume as a separate volume. The remaining member of the mirrored volume receives the drive letter that was assigned to the complete mirrored volume. The orphaned volume receives the next available drive letter or a new letter assigned to it.

You can then create a new mirrored volume from unused free space on another disk. When you restart the computer, the data from the working volume is copied to the new member of the mirrored volume.

Note In Windows NT 4.0 and earlier, mirrored volumes were known as mirror sets. Disk Management renames all mirror sets to Mirrored Volume. These mirrored volumes reside only on basic disks.

Repairing a Basic Mirrored Volume

When you follow the procedure to repair a basic mirrored volume, the status of the mirrored volume changes to Regenerating and then Healthy. If the volume does not return to the Healthy status, right-click the volume, and then click **Resynchronize Mirror**.

Note If a basic disk containing part of a mirrored volume is disconnected or fails, the status of the mirrored volume becomes Failed Redundancy and the disk status remains Online. If this happens, you can try to repair the volume.

When you repair a mirrored volume on a basic disk, Disk Management creates a new mirror on a healthy disk and then resynchronizes the new mirror.

Repairing a mirrored volume on a basic disk requires another basic disk with sufficient free space for the new mirror. If an additional disk is not available, the **Repair Volume** option is unavailable and you cannot repair the volume.

You must use a basic disk to repair a basic mirrored volume (mirror set). You cannot use a dynamic disk.

Replacing a Failed Mirror

If the disk containing part of the mirrored volume cannot be reactivated and the volume does not return to the Healthy status, replace the failed mirror with a new mirror on another disk.

- **To replace the failed mirror with a new mirror on another disk**
 1. Open Disk Management.
 2. Right-click the mirror on the missing or offline disk, and then click **Remove Mirror**. Follow the instructions on your screen.
 3. Right-click the volume to be remirrored, and then click **Add Mirror**. Follow the instructions on your screen.

To replace a mirror in the mirrored volume, you need a dynamic disk with unallocated space that is at least as large as the region to repair. If you don't have a dynamic disk with enough unallocated space, the Add Mirror command is unavailable.

Breaking a Mirrored Volume

Breaking the mirrored volume results in two independent partitions or logical drives. No information is deleted, but the data is no longer redundant. Back up the volume before breaking a mirrored volume.

Deleting Mirrored Volumes on a Basic Disk

Deleting a mirrored volume deletes all the data contained in the volume as well as the partitions that make up the volume. You can delete only entire mirrored volumes.

Resynchronizing Mirrored Volumes

Resynchronize a mirrored volume when data on one disk becomes stale. For example, if one disk of a mirrored volume is disconnected, data is written to the remaining disk, but the volume is no longer fault tolerant. If you reconnect the disk, the data on the reconnected disk is stale. To make the mirrored volume fault tolerant again, resynchronize the mirrored volume to update the information on the reconnected disk.

In most cases, mirrored volumes on dynamic disks are resynchronized automatically. However, you need to use the Resynchronize Mirror command for mirrored volumes on basic disks.

Removing Mirrored Volumes

Once you remove a mirror from a mirrored volume, that mirror becomes unallocated space; the remaining mirror becomes a simple volume and is no longer fault tolerant. All data on the removed mirror is deleted.

Recovering a RAID-5 Volume

When a member of a mirrored or RAID-5 volume fails, it becomes an orphan. The operating system determines that it can no longer be used and directs reading and writing all new data to the remaining members of the fault-tolerant volume.

When a member of a RAID-5 volume fails, you can reconstruct the data for the failed member from the remaining members. In Disk Management, select a new area of free space that is the same size as or larger than the other members of the RAID-5 volume, and then regenerate the data. If you are required to restart the computer, the volume manager reads the information from the stripes on the other member disks and then reconstructs the data of the missing member and writes it to the new member.

To regenerate a RAID-5 volume, the volume must be locked by the operating system. All network connections to the volume are lost when a volume is regenerated.

Note Do not put your page file on a RAID-5 volume because it degrades performance. If you want your page file on a fault-tolerant volume, use a mirrored volume instead.

Replacing a Stripe in the RAID-5 Volume

To replace a stripe in the RAID-5 volume, you need a dynamic disk with unallocated space that is at least as large as the stripe to repair. If you don't have a dynamic disk with enough unallocated space, the **Repair Volume** command is unavailable.

When a member of a RAID-5 volume fails in a severe manner (such as a loss of power or a hard disk failure), it becomes an orphan. If this happens, you can regenerate the data for the orphaned member from the remaining members of the RAID-5 volume.

If the RAID-5 failure is due to a power or cabling failure on a single device, you can regenerate the data within the orphaned member of the RAID-5 volume once the hardware state is restored.

Note The RAID-5 volume does not display the Healthy status in Disk Management until regeneration is complete.

Deleting a RAID-5 Volume on a Basic Disk

Deleting a RAID-5 volume deletes all the data contained in the volume as well as the partitions that make up the RAID-5 volume. You can delete only entire RAID-5 volumes.

Note In Windows NT 4.0 and earlier, RAID-5 volumes were known as stripe sets with parity. Disk Management renames all stripe sets with parity to RAID-5 Volumes. In Windows 2000, you can delete RAID-5 volumes that were created in Windows NT 4.0 or earlier, but you cannot create RAID-5 volumes on basic disks.

Repairing a RAID-5 Volume on a Basic Disk

If a basic disk containing part of a RAID-5 volume is disconnected or fails, its status becomes Failed Redundancy and the disk status remains Online. If this happens, you can try to repair the volume. The RAID-5 status of the volume should change to Regenerating and then Healthy.

When you repair a RAID-5 volume on a basic disk, Disk Management relocates part of the RAID-5 volume to a healthy disk, regenerates the parity, and then returns the status to Healthy.

Repairing a RAID-5 volume on a basic disk requires an additional basic disk with sufficient free space for part of the RAID-5 volume. If an additional disk is not available, the **Repair Volume** option is not available and you cannot repair the volume. If the disk containing part of the RAID-5 volume cannot be reactivated and the volume does not return to the Healthy status, replace the failed stripe in the RAID-5 volume.

Note You must use a basic disk to repair a basic RAID-5 volume: you cannot use a dynamic disk.

Recovering Data in Remote Storage

Remote Storage maintains data critical for operation in three areas: the reparse data that exists on each managed file; the Remote Storage database files; and the Remote Storage media. If Remote Storage data becomes corrupted or is damaged by a virus, you need to implement recovery procedures.

Using Rstore.exe

Periodically, the Remote Storage engine makes a backup of the Jet databases. Each time a file is copied or migrated to tape, these databases are automatically backed up. If required, this data might be used to restore the Jet database. The Registry Restore utility Rstore.exe is provided with Remote Storage to recover the Jet database from the backup files.

Note This data cannot simply be copied from the EngDb.bak subdirectory to the EngDb subdirectory. The files need to be restored to the same system path, including drive letter and directory structure. For example, if the system path is D:\Winnt\System32\Remotestorage\Engdb before the recovery, then after the recovery the path is still D:\Winnt\System32\Remotestorage\Engdb. This is a requirement based on the Jet database recovery mechanisms, which only recovers the Jet database to the original path location.

► **To use Rstore**

1. Using an MS-DOS window, change directories to the %SystemRoot%\System32\Remotestorage\Engdb subdirectory.
2. Delete the contents of this subdirectory.
3. Run Rstore.exe from the %SystemRoot%\System32\Remotestorage\Engdb subdirectory. Rstore.exe requires one parameter which identifies the location of the backup subdirectory. Typically, the following command is entered:

Rstore %SystemRoot%\System32\Remotestorage\Engdb.bak

Restoring the Remote Storage and Removable Storage Databases

There are two reasons for restoring the Remote Storage database, each with its own restore procedure. Use the appropriate method to restore the Remote Storage database in the following circumstances:

- After completely reinstalling Windows 2000, you need to restore the Remote Storage database files before you can recall files from offline storage.
- The Remote Storage database is damaged.

Note If you try to access a file in offline storage when the Remote Storage service is not installed, you might receive the following error message:

path and file name The file can not be accessed by the system.

If Remote Storage is installed but does not start you might receive the following error message:

Path and file name The remote storage service was not able to recall the file.

Restoring the Removable Storage Databases

After completely reinstalling Windows 2000, restore the Removable Storage databases before you restore the Remote Storage database. Each time Remote Storage migrates data to tape, these databases are automatically backed up to the media containing the migrated data. It is recommended that the databases on this media be used since they will contain the most recent copy of the Removable Storage database. Use the following procedure to restore the Removable Storage databases.

Note For the following procedure, you need to reinstall Windows 2000 into the same folder and drive previously used. If Windows 2000 is installed to a different folder, the restore operation cannot return the databases to their original location.

► **To restore the Removable Storage databases**

Caution This procedure can cause you to lose changes to the Removable Storage database made after Remote Storage was backed up and before it was restored.

1. Verify that your tape or storage device is online and functioning. Start the Computer Management snap-in by right-clicking **My Computer**. Click **Manage**, double-click the **Storage** branch to expand it, and then click **Removable Storage**.
2. Open the **Media** pools and look in the **Import** pool. Locate the most recent tape used to store the Remote Storage migrated files. The default name for Remote Storage media is "RS" appended with the computer name and an incremental number (for example, "RS-MachineX-1"). The media with the highest number contains the most recent database backup. If the Remote Storage media spans two or more tapes, catalog these tapes using Backup (temporarily move these tapes to the **NTBackup Media** pool) and check the dates of the Remote Storage databases. Use the one with the most recent date.
3. Move this media to the **NTbackup Media** pool. If the pool does not exist, start Backup, and it is created automatically.
4. Use Backup to catalog the tape to find the latest copy of the Removable Storage and Remote Storage databases. These databases are stored on tape in the folders %windir%\system32\Ntmsdata and %windir%\system32\RemoteStorage. Check the dates of the files to determine the most recent copies.
5. Select the most current versions of the NtmsData and RemoteStorage folders to be restored. Make sure that all files below these sub-folders are also selected.

6. In the **Restore files to** box, click **alternate location**, and then click the drive that contains the Windows folder.

Caution If the previous step is not performed, the databases are restored to the Remote Storage managed volume instead of the Windows 2000 operating system partition.

7. Click **Start Restore**, and then click **Advanced**. Click **Restore Removable Storage Database**, click **OK**, and then click **OK**.
8. After this process finishes, restart your computer.

Restoring the Remote Storage Database After Completely Reinstalling Windows 2000

Before restoring the Remote Storage database, reinstall Windows 2000 to the same drive and folder as the previous installation. During Setup, do not add the Remote Storage component. If this component was added accidentally or automatically, remove it, and then restart your computer.

Important The following procedure assumes that you have completely reinstalled Windows 2000; that volumes that contain Remote Storage managed data are still intact; and that you have already performed the procedure to restore the Removable Storage databases.

► To restore the Remote Storage database after completely reinstalling Windows 2000

1. Start the Removable Storage snap-in and verify that the databases have been restored. You can do this by looking to see if all of your media pools are present and the media are in their appropriate pools.
2. In Control Panel, use **Add/Remove Programs** to add Remote Storage .
3. Restart your computer, log on, and then using the Computer Management snap-in, expand the **Services And Applications** branch, and then click **Services**. Verify that the following services are stopped:
 - Remote Storage Engine
 - Remote Storage File
 - Remote Storage Media
 - Remote Storage Notification
4. At a command prompt, change to the %SystemRoot%\System32\RemoteStorage\Engdb folder, and then verify that this folder is empty by moving the files to another folder.

5. Use the **Rstore.exe** tool to run the following command from the Engdb folder.
Type:
Rstore %systemroot%\system32\RemoteStorage\engdb.bak
6. In the Computer Management snap-in, expand **Services And Applications**, and then click **Services**. Locate and start the following services:
 - Remote Storage Engine
 - Remote Storage File
 - Remote Storage Media
7. Open the Remote Storage snap-in and verify that your managed volumes appear and that all settings are correct. You may also want to test by recalling a few of the migrated files before putting the server back into production.

Restoring a Damaged Remote Storage Database

The following procedure assumes that the Removable Storage database is intact and that you are only restoring the Remote Storage database. For detailed information about restoring the Removable Storage database, see “Restoring the Removable Storage Databases” earlier in this chapter.

► To restore a damaged Remote Storage database

1. In the Computer Management snap-in, expand **Services And Applications**, and then click **Services**. Verify that the following services are stopped:
 - Remote Storage Engine
 - Remote Storage File
 - Remote Storage Media
 - Remote Storage Notification
2. Using Removable Storage, open the **Media** pools and view in the **Import** pool. Locate the most recent tape used to store the Remote Storage migrated files. The default name for Remote Storage media is "RS" appended with the computer name and an incremental number. For example, RS-MachineX-1. The media with the highest number contains the most recent backup of the databases.
3. Move this media to the **NTbackup** media pool. If the pool does not exist, start Backup.

4. Using Backup, catalog the tape to find the latest copy of the Remote Storage database on tape in the %Windir%\System32\RemoteStorage folder. Check the dates of the files to find the most recent copies.

Note If the Remote Storage media spans two or more tapes, catalog these tapes using Backup (temporarily move these tapes to the **NTBackup Media** pool). Check the dates of the Remote Storage databases and use the most recent one.

5. Select the most current RemoteStorage folder to be restored, and make sure that all files under this folder are also selected.
6. In the **Restore files to** dialog box, click **Alternate location**, and then click the drive that contains the Windows folder.

Caution If the previous step is not performed, the databases are restored to the Remote Storage managed volume instead of the Windows 2000 operating system partition.

7. After the restoration finishes, at the command prompt, type:
%systemroot%\system32\RemoteStorage\engdb

Note Make sure that this folder is empty by moving any existing files to another folder.

8. Use the **Rstore.exe** tool to run the following command from the Engdb folder.
Type:
Rstore %systemroot%\system32\RemoteStorage\engdb.bak
9. After this command finishes, place the Remote Storage media used during the restoration in the RemoteStorage media pool.
10. In the Computer Management snap-in, expand **Services And Applications**, and then click **Services**. Locate and start the following services:
 - Remote Storage Engine
 - Remote Storage File
 - Remote Storage Media
11. Open the Remote Storage snap-in and verify that your managed volumes appear and that all settings are correct. You might also want to test by recalling some migrated files before putting the server back into production.

Recovering Managed Files

Remote Storage data is stored in the MTF format. To recover managed files from the system backup, perform the same restore operations that you would use to restore files that are not managed by Remote Storage. Remote Storage detects when restore operations have occurred and schedules a validate job to run against the restored volume. The restore function on a Backup tape restores the reparse points and all files that are not managed by Remote Storage. By default, when Backup backs up files in Remote Storage, the reparse data (not the full file) is backed up. For this reason you still need the Remote Storage media with the Remote Storage databases to recall the files from the reparse point and fully recover a managed volume.

If the volume was destroyed and you have backups of the reparse point data, you can recover by either restoring the reparse point data from tape or restoring the Remote Storage and Removable Storage databases from the Remote Storage media. For more information, see “Restoring the Remote Storage Database” earlier in this chapter.

Caution As a last resort (for example, if remote storage recovery was not successful), use Backup to restore data from the Remote Storage media.

Using Backup to restore data from the Remote Storage media can cause problems under the following circumstances:

- More than one version of the file exists on the Remote Storage media. For example, if a file was migrated, recalled, modified, and then migrated again, the wrong version of the file might be restored.
 - A user has deleted a file that no longer needs to be archived. The file still resides on the tape even though the reparse point to it is severed.
-

► To recover Remote Storage files

Remote Storage does not recall files while they are being recovered.

1. Open the Removable Storage snap-in, and then locate the Remote Storage tapes in the import media pool or the Remote Storage pool.
2. Open Backup to create a media pool in Removable Storage.

3. Right-click the appropriate media, click **Copy**, right-click the Backup pool, and then click **Paste**.

–Or–

Highlight the media, and then drag it to the Backup pool.

Note Backup needs to have been opened before a pool can be created in Removable Storage. Backup then needs to be restarted before it can recognize the media that is pasted into its pool. This needs to be done with care, because this temporarily prevents recalls from occurring if Remote Storage is installed and running.

4. After recovering the needed files, cut and paste the media back into the Remote Storage media pool.

Use the Backup restore function to catalog and view the available directories and files to be restored. The tape contains the directory names and the date of the Remote Storage and Removable Storage database files.

Each set needs to be individually cataloged to produce a listing of all files on the tape. All files and directories that were managed are visible in the right pane after expanding the directory associated with the file. The restore function allows the restoration of files to the same directory as well as to alternative locations. If you want the file to be able to be recalled from the managed placeholder, restore it to an alternative location. The restore operation returns the file to the state that the file was in at time of management.

Recovering from Bad Media

Tape media can wear out, become unstable, or become unusable. If this happens, you can make a media copy and recover using the media copy set. This process ensures that the managed data is safe for a longer period of time. If you cannot make a media copy because only one drive is available or no tapes are available, set the write-protect tab on the medium. Only use this procedure if the medium is unstable or unusable.

If a master medium becomes unusable, use the following procedure to recreate the master media for Remote Storage recall use.

► **To recreate the master media**

- In the Remote Storage snap-in, on the individual media property page, submit a recreate master from the recovery page, using the latest media copy.

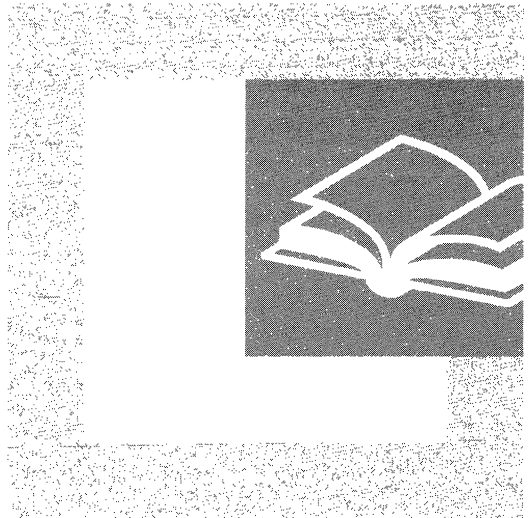
There is a potential for lost data because the copy was older than the master that was in place. This allows for the recovery of the data up to the point where the media copy was last updated. At this point, the original master is marked “bad” and all data is accessed through the recreated master.

Additional Resources

- For more information about using tools such as the ERD and the Recovery Console, see Windows 2000 Server Help.

P A R T 4

Troubleshooting



Troubleshooting strategies include methods, checklists, and hints to find and correct problems with a computer running Microsoft® Windows® 2000. A wide range of troubleshooting tools are included with the operating system and the *Windows 2000 Resource Kit*. Part 4 includes general troubleshooting data and information that can be used to troubleshoot specific problems.

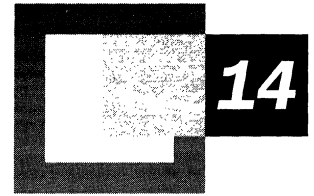
In This Part

Troubleshooting Strategies 563

Startup Process 613

Windows 2000 Stop Messages 637

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

Technical Support and Services	565
Troubleshooting Tools for Windows 2000	567
Troubleshooting Options	580
Troubleshooting Suggestions	595
Troubleshooting Techniques	597
Troubleshooting Hardware Problems	605
Troubleshooting Specific Problems	607

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 processing 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.

(continued)

Table 14.3 Software Environment *(continued)*

Section	Definition
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 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 V1.1 is 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. . . . . : ntcorpdcl.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 <i>adapter</i>	Displays all the DHCP class IDs allowed for the adapter specified.
/setclassid <i>adapter</i>	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 log in 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.

ErrorControlEntry

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.

TypeEntry

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.

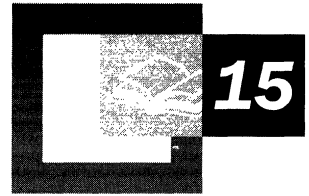
You can also use the undocked hardware profile to set a different video resolution for your portable computer. For example, the Original Configuration can have the video resolution set to 1024x768 to run on your monitor, and you can change your undocked configuration to use a resolution of 640x480 or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

CHAPTER 15

Startup Process



Understanding each step in the startup process is important for troubleshooting problems that can occur while starting up or that can prevent the computer from starting at all. Microsoft® Windows® 2000 also provides tools that you can use to identify and repair startup problems when they occur.

In This Chapter

Windows 2000 Startup Requirements 615

Starting Windows 2000 615

Troubleshooting Startup Problems 625

Options to Use When a System Does Not Start 629

Related Information in the Resource Kit

- For more information about recovery, see “Repair, Recovery, and Restore” in this book.
- For more information about using the registry to troubleshoot problems, see the Technical Reference to the Windows 2000 Registry (Regentry.chm) on the *Microsoft® Windows® 2000 Resource Kit* companion CD.

Windows 2000 Startup Requirements

The data contained in the system files is required to start the Windows 2000 operating system. During the startup process, various screens and messages are displayed on your screen.

The Windows 2000 startup process requires the following steps:

1. Power-on self test (POST) processing
2. Initial startup process
3. Bootstrap loader process
4. Selecting the operating system
5. Detecting hardware
6. Selecting a configuration
7. Loading and initializing the kernel (Ntoskrnl.exe)
8. Logging on

You can begin startup by one of the following methods:

- Turn on the computer.
- In the **Shut Down Windows** dialog box, select **Restart**.

Important Windows 2000 might not start or operate correctly if any hardware components do not initialize correctly. Startup fails if any of the files that are required to start Windows 2000 are not present in the correct folder, or if any of the files has been corrupted.

When you see **Press Ctrl+Alt+Delete to begin** in the **Welcome to Windows** dialog box, the loading and much of the initialization of Windows 2000 is complete. However, startup is complete only when you can successfully log on using the **Welcome to Windows** dialog box.

Starting Windows 2000

Table 15.1 describes specific files that are required to start Windows 2000.

Table 15.1 Files Required to Start Windows 2000

File	Location
NTLDR	Active Partition
Boot.ini	Active Partition
Bootsect.dos (required only for multiple booting)	Active Partition
Ntdetect.com	Active Partition
Ntbootdd.sys (Required only if you are using a SCSI-controlled boot partition, and the SCSI adapter does not have a SCSI BIOS enabled).	Active Partition
Ntoskrnl.exe	%SystemRoot%\System32
Hal.dll	%SystemRoot%\System32
SYSTEM key	%SystemRoot%\System32\Config
Device drivers	%SystemRoot%\System32\Drivers

Note The string %SystemRoot% is replaced by the directory in the boot partition that contains the Windows 2000 system files.

Power-On Self Test Process

When you turn on or restart a computer, it begins a POST routine. The POST routine determines the available amount of real memory and verifies the presence of required hardware components, such as the keyboard.

After the computer runs its POST routine, each adapter card with a basic input/output system (BIOS) runs its own POST routine. The computer and adapter card manufacturers determine what appears on the screen during POST processing.

Initial Startup Process

After the successful execution of the POST, the system BIOS then checks the first hard disk that is powered up.

When the hard disk is the startup disk, the system BIOS reads the master boot record (MBR) and loads it into memory. The system BIOS then transfers the execution of the startup process to the MBR. After the MBR loads a copy of the active partition's boot sector into memory, the boot sector code starts the operating system as defined by the operating system.

Bootstrap Loader Process

NTLDR is the bootstrap loader for the Windows 2000 operating system, and is responsible for the following operations:

- Enabling the user to select an operating system to start.
- Loading the operating system files from the boot partition.
- Controlling the operating system selection process and hardware detection prior to the Windows 2000 kernel initialization.

Before you can start the operating system, NTLDR and the following files must be in the active partition of your startup disk:

- Ntdetect.com
- Boot.ini
- Bootsect.dos (if you plan to boot more than one operating system on your computer)

Signature() Syntax

The signature() syntax is equivalent to the SCSI() syntax, but is used instead to support the Plug and Play architecture in Windows 2000. The SCSI controller number might vary each time you start Windows 2000, especially if you add new SCSI controller hardware after Setup is finished. Using the signature() syntax instructs NTLDR to locate the drive whose disk signature matches the value in the parentheses, no matter which SCSI controller number the drive is connected to. The following is an example of a Boot.ini file with a signature() entry:

```
signature(8b467c12)disk(1)rdisk(0)partition(2)\winnt="description"
```

Note If multiple preexisting Boot.ini entries use scsi() they are maintained and not converted to signature() syntax.

Advanced RISC Computing (ARC) path entries in the Boot.ini file start with "signature()" syntax in the following situations:

- The partition on which you installed Windows 2000 is larger than 7.8 gigabytes (GB) in size, or the ending cylinder number is higher than 1024 for that partition.
- The drive on which you installed Windows 2000 is connected to a SCSI controller whose BIOS is disabled, so INT13 BIOS calls cannot be used during the startup process.

Because the `signature()` syntax replaces the `scsi()` syntax, the same requirement applies in that a file named `Ntbootdd.sys` is required in the root folder of the system partition to address the SCSI controller at startup. This file is the specific SCSI miniport device driver for the SCSI adapter from which you are booting, renamed to `Ntbootdd.sys`, and placed in the root folder of the system drive.

Note If multiple pre-existing `Boot.ini` entries use `scsi()` syntax, they are maintained and not converted to `signature()` syntax.

For more information about `signature()` syntax, see the Microsoft Knowledge Base link on the Web Resources page at <http://windows.microsoft.com/windows2000/reskit/webresources>.

NTLDR

When NTLDR runs, it clears the screen and displays the bootstrap loader message:

OS Loader V5.0

NTLDR then performs the following steps:

- Switches the processor into the 32-bit flat memory mode. When a computer first starts, it runs in real mode, like an 8088 or 8086 CPU. Because NTLDR is mostly a 32-bit program, it must switch the processor to 32-bit flat memory mode before it can perform any other functions.
- Starts the appropriate minifile system. The code to access files on file allocation table (FAT) file system and NTFS file system volumes is built into NTLDR. This code enables NTLDR to read, access, and copy files.
- Reads the `Boot.ini` file, and displays the operating system selections. This screen is referred to as the bootstrap loader screen.
- Allows you to select an operating system from the bootstrap loader screen.
If you select an operating system other than Windows 2000, NTLDR loads `Bootsect.dos` and passes control to it. The operating system then starts up as normal, because `Bootsect.dos` contains the boot sector that was on the primary partition before you installed Windows 2000.
If you select Windows 2000, NTLDR runs `Ntdetect.com` to gather information about currently installed hardware.
- Allows you to choose between starting the computer in the configuration in use when Windows 2000 was last shut down (Default), or selecting troubleshooting and advanced startup options by pressing F8. For more information on safe mode, see “Safe Mode” later in this chapter.
- Loads and starts `Ntoskrnl.exe`. NTLDR passes the hardware information collected by `Ntdetect.com` to `Ntoskrnl.exe`.

Selecting the Operating System

NTLDR displays the bootstrap loader screen, where you can select an operating system to start. This screen is based upon the information in the Boot.ini file. The screen display is similar to the following:

Please select the operating system to start:

Windows 2000 Advanced Server

Use ↑ and ↓ to move the highlight to your choice.

Press ENTER to choose.

Seconds until highlighted choice will be started automatically: 29

For troubleshooting and advanced startup options for Windows 2000, press F8.

If you do not select an entry before the counter reaches zero, NTLDR loads the operating system specified by the default parameter in the Boot.ini file. Windows 2000 Setup sets the default entry to the most recently installed copy of Microsoft® Windows NT® version 4.0 or earlier. You can edit the Boot.ini file if you want to change the default to either an earlier version of Windows 2000 or to another operating system.

Windows 2000 Setup places the Boot.ini file in the active partition. NTLDR uses information in the Boot.ini file to display the bootstrap loader screen from which you select the operating system.

The following is an example of a Boot.ini file:

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINNT
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Windows 2000 Server"
/fastdetect
```

The Boot.ini file has two sections, [boot loader] and [operating systems]. You can use the parameters in the [boot loader] section to customize startup, as described in Table 15.2.

Table 15.2 Bootstrap Loader Parameters

Parameter	Description
Time-out	<p>The time that the user has to select an operating system from the bootstrap loader screen before NTLDR loads the default operating system.</p> <p>If the time-out value is 0, NTLDR immediately starts the default operating system without displaying the bootstrap loader screen.</p> <p>If you set this value to –1, NTLDR waits indefinitely for you to make a selection. You must edit the Boot.ini file directly because –1 is an illegal value for the System option in Control Panel.</p>
Default	<p>The ARC pathname to the default operating system.</p>

Each entry in the [operating systems] section includes the ARC pathname to the boot partition for the operating system, the string to display on the bootstrap loader screen, and optional parameters. The bootstrap loader screen presented earlier in this chapter is an example of the use of this section of the Boot.ini file.

You can use the Boot.ini file to start multiple versions of the Windows 2000 operating system, as well as one other operating system, including Microsoft® MS-DOS®, Microsoft® Windows® 95, and Microsoft® Windows® 98.

Boot.ini Switches

The switches listed in Table 15.3, which can be added to the end of the [operating system] section of the Boot.ini file, are not case sensitive. For more information about the /MAXMEM and /SOS switches, see “Problem Occurs After the Bootstrap Loader Starts” later in this chapter. The switch you want to add must be placed on a separate line of the Boot.ini file.

Table 15.3 Boot.ini Switches

Switch	Description
/BASEVIDEO	<p>The computer starts up using the standard VGA video driver. If you have installed a new video driver and it is not working correctly, you can select the Windows 2000 entry with this switch to start the computer and change to a different driver.</p>
/BAUDRATE=nnnn	<p>Specifies the baud rate to be used for debugging. The default baud rate is 9600 if a modem is attached, and 19200 for a null-modem cable. Including this switch in the Boot.ini file causes the /DEBUG switch to activate.</p>

(continued)

Table 15.3 Boot.ini Switches *(continued)*

Switch	Description
/CRASHDEBUG	The debugger is loaded when you start Windows 2000, but remains inactive unless a kernel error occurs. This switch is useful if you are experiencing random kernel errors.
/DEBUG	The debugger is loaded when you start Windows NT, and can be activated at any time by a host debugger connected to the computer. Use this switch when you are debugging problems that are regularly reproducible.
/DEBUGPORT= comx	Specifies the communications port to use for debugging, where <i>x</i> is the communications port that you want to use. Including this switch in the Boot.ini file causes the /DEBUG switch to activate.
/MAXMEM:n	Specifies the maximum amount of RAM that Windows 2000 can use. Use this switch if you suspect that a memory chip is bad.
/NODEBUG	No debugging information is being used.
NUMPROC=x	Allows you to force a multiprocessor computer to start up with < <i>n</i> processors.
/FASTDETECT =[COMx COMx,y,z,...]	Turns off serial and bus mouse detection in NTDETECT. Use this switch if you have a component other than a mouse attached to a serial port during the startup process. If you use /FASTDETECT without specifying a communications port, serial mouse detection is disabled on all communications ports.
/SOS	Displays the device driver names as they are being loaded. Use this switch when startup fails (while loading drivers), to determine which driver is triggering the failure.
/PAE	Specify the /PAE switch with the corresponding entry in Boot.ini to allow a computer that supports physical address extension (PAE) mode to start normally. In safe mode, the computer starts using normal kernels even if the /PAE switch is specified.

Editing Boot.ini

When you install Windows 2000, the read-only, system, and hidden attributes of the Boot.ini file are set. Regardless of the value of these attributes, you can edit the timeout and default parameters in the Boot.ini file using the **System** option in Control Panel.

To edit the Boot.ini file with a text editor, you need to make the file visible and turn off the read-only attribute. You can change file attributes using My Computer or at the command prompt.

► **To change file attributes using My Computer**

1. On the **Tools** menu, click **Folder Options**.
2. On the **View** tab, double-click **Hidden files and folders**.
3. Select either **Do not show hidden files and folders** or **Show hidden files and folders**.
4. Click **OK**.

Important If you change the path to the Windows 2000 boot partition, make sure to edit both the default path and operating system path entries. If you change one but not the other, a new choice is designated as the default selection and added to the bootstrap loader screen.

Detecting Hardware

Ntdetect.com detects installed hardware during the Windows 2000 startup sequence. Ntdetect.com passes this information to NTLDR and places a list in the registry. Ntdetect.com detects the following components:

- Computer ID
- Bus/adaptor type
- SCSI adapters
- Video adapters
- Keyboard
- Communication ports
- Parallel ports
- Floppy disks
- Mouse/pointing device
- Floating-point coprocessor

Ntdetect.com runs after you select an operating system on the bootstrap loader screen (or the timer times out). NTLDR has started when you see the message:

Starting Windows . . .

followed by a bar graph. When the bar graph becomes solid, the text mode switches to the graphical mode, and the Microsoft® Windows® 2000 Server Family screen is displayed.

Loading and Initializing the Kernel

After you choose a hardware profile or configuration, or when NTLDR automatically makes the selection for you, the kernel load phase of the Windows 2000 startup process begins. During this process, NTLDR performs the following operations:

- Loads the Windows 2000 kernel (Ntoskrnl.exe) and the hardware abstraction layer (Hal.dll) into memory (NTLDR does not initialize these programs yet).
- Loads the registry key HKEY_LOCAL_MACHINE\SYSTEM from %SystemRoot%\System32\Config\System.
- Selects a Configuration. The first hardware profile is highlighted by default. If you have created other hardware profiles, use the DOWN ARROW key to select the one that you want to use.
- Selects the control set that it uses to initialize the computer.
- Loads device drivers that have a Start value of 0x0.

Important Do not change the values in the folder %SystemRoot%\System32\Config\System.

For more information about hardware profiles, use see Windows 2000 Server Help.

Selecting the Control Set

The values of the entries in the HKEY_LOCAL_MACHINE\SYSTEM\Select subkey determine which control set to use.

If you did not press F8 when the OS Loader V5.0 screen was displayed, or if you have only one hardware profile, NTLDR uses the control set identified by the value of the Default entry in the subkey HKEY_LOCAL_MACHINE\SYSTEM\Select. However, if you chose **Last Known Good Configuration** from the **Windows 2000 Advanced Options** menu that is displayed when you pressed F8 and you selected **Last Known Good Configuration** from the **Hardware Profile/Configuration Recovery** menu, the value of the LastKnownGood entry in the subkey HKEY_LOCAL_MACHINE\SYSTEM\Select specifies the control set.

Based on your actions and the value of the corresponding Select subkey entry, NTLDR determines which ControlSet00x to use. NTLDR sets the Current value of the subkey HKEY_LOCAL_MACHINE\SYSTEM\Select to the number of the control set it will use.

Note The two registry editors, Regedt32.exe and Regedit.exe, are included on the Windows 2000 Setup CD. You can use either one to view the registry. For more information about the registry, see the Technical Reference to the Registry on the *Windows 2000 Resource Kit* companion CD.

Loading Device Drivers

NTLDR scans the registry subkey HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services for device drivers with a Start value of 0x0. This value indicates that the device drivers should be loaded but not initialized. Device drivers are loaded into memory by using BIOS calls in real mode or by Ntbootdd.sys.

Next, Ntoskrnl.exe initializes the kernel. If the Boot.ini ARC path entry contains the /SOS switch, text similar to the following is displayed:

```
Microsoft (R) Windows 2000 (TM) Version 5.0 (Build xxxx)
1 System Processor (16 MB Memory)
```

Upon successful initialization, Ntoskrnl.exe:

- Creates the Clone control set by making a copy of the control set pointed to by the value of Current.
- Creates the HKEY_LOCAL_MACHINE\HARDWARE key using the information that was passed from NTLDR. This key contains the hardware data that is detected and computed at each system startup. The data includes information about hardware components on the system board and about the interrupts hooked by specific hardware devices.

Initializing Device Drivers

Ntoskrnl.exe initializes the low-level device drivers with a start value of 0x0, which were loaded during the Kernel load phase. Ntoskrnl.exe then scans the subkey HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services for device drivers with a Start value of 0x1, which are initialized as soon as they are loaded. They are not loaded by BIOS, but by the device drivers loaded during the kernel load phase and that have already been initialized.

Error Processing

If an error occurs during the loading and initializing of a device driver, the action taken is based on the value of the **ErrorControl** entry in the registry subkey `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services` for the device driver that has a problem.

Logging On to Windows 2000

The Windows 2000 subsystem automatically starts `Winlogon.exe`, which starts the Local Security Administration, `Lsass.exe`. The **Welcome to Windows** dialog box appears, containing the text **Press Ctrl+Alt+Delete to begin**. Although Windows 2000 might still be initializing network device drivers, you can log on.

Next, the Service Controller (`Screg.exe`) checks the subkey `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services` for services with a `Start` value of `0x2`, which are loaded automatically.

Services are loaded in parallel, based on their dependencies. The dependencies are described in the **DependOnGroup** and **DependOnService** entries in the subkey `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`.

Note Windows 2000 startup is not considered complete until a user successfully logs on to the system. After a successful logon, the Clone control set is copied to the LastKnownGood control set.

Troubleshooting Startup Problems

If your computer fails to complete startup, it might stop, or it might display an error message. This section discusses ways to troubleshoot problems that can prevent Windows 2000 from starting.

The first step in figuring out what causes a startup problem is to determine if the problem occurs before or after the operating system takes control. If you do not see the bootstrap loader screen, the problem might be due to hardware failure. Possible causes also include a faulty MBR or partition table, or a damaged boot sector.

Damage can have several causes, including viruses. Viruses use BIOS calls to install themselves, so they are operating-system independent. Windows 2000 traps BIOS calls while it is running, but cannot protect itself when the computer is multiple-booted by using MS-DOS. For more information about protecting your computer from viruses and recovering from problems with viruses, see the Microsoft Knowledge Base link on the Web Resources page at <http://windows.microsoft.com/windows2000/reskit/webresources>.

If the problem occurs after selecting Windows 2000 from the bootstrap loader screen, files that are needed by the operating system might be missing or corrupt. For more information, see “Options to Use When a System Does Not Start” later in this chapter.

Problem Occurs Before the Bootstrap Loader Starts

This section describes the problems that might occur between the time you turn the computer on until you see the bootstrap loader screen. Symptoms of problems in this group include the following:

- The computer hangs immediately after the power-on self test (POST).
- You do not see the bootstrap loader screen.
- You receive messages such as:
 - Missing operating system.
 - A disk read error occurred.
 - Insert a system diskette and restart the system.
 - Invalid partition table.
 - Hard disk error.
 - Hard disk absent/failed.

Table 15.4 lists symptoms, possible trouble causes and sources of more detailed information.

Table 15.4 Startup Problems

If You See Messages About or Suspect a Problem with . . .	Possible Problem	Source for More Information
POST routine	The POST routine is inaccessible.	“Hardware Problems” later in this chapter.
System partition	There is no system partition on the first hard disk.	“Disks Concepts and Troubleshooting” in this book.
Master boot record	The MBR is corrupt.	“Disks Concepts and Troubleshooting” in this book.
Partition table	The partition table is invalid.	“Disks Concepts and Troubleshooting” in this book.
Multiple-booting between Windows 2000 and MS-DOS	Bootsect.dos must be restored.	Windows 2000 Server Help.

(continued)

Table 15.4 Startup Problems *(continued)*

If You See Messages About or Suspect a Problem with . . .	Possible Problem	Source for More Information
Boot.ini	The Boot.ini file is missing.	“Problem Occurs after the Bootstrap Loader Starts” later in this chapter.
Bootstrap loader screen	NTLDR, is missing or corrupt.	“Problem Occurs after the Bootstrap Loader Starts” later in this chapter.
CMOS	The CMOS is corrupt, or the CMOS battery is run down.	“Disks Concepts and Troubleshooting” in this book.
Hardware	If you have installed new hardware or new drivers, they could be causing the problem, or a hardware component has malfunctioned.	“Hardware Problems” later in this chapter.

You might not be able to start your computer to troubleshoot the problem. If all of your volumes are formatted by using NTFS, you cannot use MS-DOS-based utilities.

Problem Occurs After the Bootstrap Loader Starts

This section describes problems that might occur after NTLDR starts executing until you successfully log on to Windows 2000.

Using Checked Version of NTDETECT

NTDETECT detects installed hardware components.

There is a debug version of Ntdetect.com on the *Windows 2000 Resource Kit* companion CD, called Ntdetect.chk. If Ntdetect.com fails to detect all of the hardware that you think it should find, you can use Ntdetect.chk to help isolate the problem. Typically, a mouse or a disk controller is the cause of the problem.

► To use the debug version of Ntdetect:

1. Rename Ntdetect.com to Ntdetect.bak in the root folder of your system partition.
2. Copy Ntdetect.chk from Support\Debug\I386 to the root folder.
3. Rename Ntdetect.chk to Ntdetect.com.

The utility Installld, included on the *Windows 2000 Resource Kit* companion CD, performs the same functions.

Ntdetect.com has the hidden, system, and read-only attributes set when you install Windows 2000. Clear these attributes to make the file visible.

After Ntdetect.chk displays information about the components, press ENTER to continue. Ntdetect.chk next displays information about the current nodes for the controllers and peripherals. Press ENTER at the end of each screen.

When you have finished using Ntdetect.chk, rename Ntdetect.com to Ntdetect.chk and rename Ntdetect.bak to Ntdetect.com.

Using the /MAXMEM Switch

The Boot.ini file has a /MAXMEM switch which you can use specify the maximum amount of RAM that Windows 2000 can use. You can use this switch to troubleshoot memory parity errors, mismatched SIMM speeds, and other memory-related problems. To use this switch, the memory must be contiguous. Never specify a value less than 32 for Windows 2000 Professional.

Include this switch at the end of the ARC path specified in the [operating systems] section of the Boot.ini file. In the following example Windows 2000 Professional is restricted to using only the first 32 MB RAM.

```
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\winnt="Windows 2000 Professional"
/fastdetect /MAXMEM=32
```

Note For Windows 2000 Server, use a minimum of 64 MB.

For more information about troubleshooting memory problems, see “Troubleshooting Strategies” in this book.

Using the /SOS Switch

You can add the /SOS switch to the Boot.ini file to have NTLDR display the kernel and device driver names while they are being loaded. Use this switch if Windows 2000 does not start up and you think a driver is missing or corrupted. For information about changing Boot.ini switches, see “Boot.ini Switches” earlier in this chapter.

Hardware Problems

If a device fails to initialize during the POST routine, you might not be able to gain access to it. If you have not changed or added devices since the last startup, check for the following:

- Controller cards are seated properly.
- Cables are properly connected.
- Disks are turned on.

If you have changed hardware or device drivers since the last startup, the problem might be with the new configuration. You should check that:

- SCSI devices are terminated properly.
- There are no IRQ conflicts.
- The BIOS is enabled on only the first SCSI controller (if at all).

During the startup process, the **Hardware Profile/Configuration Recovery** menu provides options for using alternative configurations. If you have checked the above items and Windows 2000 does not complete startup, try using one of the other configuration options listed in the **Hardware Profile/Configuration Recovery** menu.

For more information about hardware problems, see “Troubleshooting Strategies” in this book, or see the Microsoft Knowledge Base link on the Web Resources page at <http://windows.microsoft.com/windows2000/reskit/webresources>.

Note On NTFS volumes, you need to use Windows 2000-based utilities, such as DiskProbe, to examine information on the volume. DiskProbe is a low-level disk editor that you can use to examine and change individual disk sectors.

If you use the Windows 2000 Setup floppy disks, try using the following utilities:

- The Computer Management snap-in in Administrative Tools where you can view system information.
- The DiskProbe tool, a low-level disk editor that you can use to examine and change individual disk sectors.

Options to Use When a System Does Not Start

Windows 2000 provides a variety of options that you can use when a computer does not start, including safe mode, the Recovery Console, and the Emergency Repair Disk (ERD). You can use safe mode to start the computer with only minimal necessary services. Safe mode options, including Last Known Good Configuration, are especially useful if a newly-installed driver is causing the problems.

If safe mode does not start the computer, you can use the Recovery Console. Using the Recovery Console is recommended only for advanced users or administrators. You can access the Recovery Console to start the system by using the Windows 2000 Setup CD or the Setup floppy disks that you created from the CD. The Recovery Console is a command-line interface that allows you to perform tasks such as starting and stopping services and accessing the local drive.

The ERD provides another option if safe mode and the Recovery Console do not start the system. If you have already created an ERD, you can start the system with the Windows 2000 Setup CD or the Setup floppy disks, and then use the ERD to restore core system files.

Safe Mode

Safe mode is a diagnostic tool for troubleshooting problems that can occur with starting and running Windows 2000. It is only accessible when the computer is started. As part of the **Windows 2000 Advanced Options** menu, safe mode allows the user to specifically control how the computer starts Windows 2000.

If the computer fails to startup properly, on the next restart, Windows 2000 displays the **Windows 2000 Advanced Options** menu, containing several startup troubleshooting options. You can also manually prompt Windows 2000 to display the **Windows 2000 Advanced Options** menu.

When starting Windows 2000 in safe mode, only essential drivers and system services are loaded, including the mouse, keyboard, CD-ROM and standard VGA device drivers, and the Event Log, Plug and Play, Remote Procedure Call (RPC), and the Logical Disk Manager system services. This makes safe mode useful for isolating and resolving error conditions that are caused by faulty applications, system services, and device drivers that are started automatically.

Although a computer started in safe mode has only a minimum of necessary services, you can access all partitions on functioning physical disks. Use safe mode for system startup in situations such as the following:

- If Windows 2000 seems to stall for an extended period of time.
- If Windows 2000 does not work correctly or has unexpected results.
- If your video display does not work correctly.
- If your computer suddenly slows down.
- If you need to test an intermittent error condition.

Once in safe mode, you can disable or delete a system service, a device driver, or automatically started application that is preventing the computer from starting normally.

To use a safe mode option, restart your computer, and then press F8 when you see the **Boot** menu. The **Windows 2000 Advanced Options** menu appears:

Windows 2000 Advanced Options Menu

Please select an option:

Safe Mode

Safe Mode with Networking

Safe Mode With Command Prompt

Enable Boot Logging

Enable VGA Mode

Last Known Good Configuration

Directory Services Restore Mode (Windows 2000 domain controllers only)

Debugging Mode

Boot Normally

Use ↑ and ↓ to move the highlight to your choice.

Press Enter to choose.

Select an option, and then press ENTER. The **Boot** menu is displayed again, with the words “Safe Mode” displayed in red at the bottom. Select the operating system installation that you want to start, and then press ENTER.

Important When you select the operating system installation to start, you must choose a version of Windows 2000. Do not choose another Windows-based operating system.

When you use one of the safe mode options the environment variable Safeboot_Option is set to either Network or Minimal.

The default Microsoft VGA driver is used for display (640 x 480 x 16 colors). You must log on in all modes (either by a domain or the local SAM, depending on which safe mode option you choose).

Table 15.5 describes the **Windows 2000 Advanced Options** menu.

Table 15.5 Windows 2000 Advanced Options Menu

Option	Description
Safe Mode (Safeboot_Option=Minimal)	Starts Windows 2000 using basic files and drivers only, without networking. The drivers and files used are for mouse, monitor, keyboard, mass storage, base video, and default system services.
Safe Mode with Networking (Safeboot_Option=Network)	Similar to standard safe mode, but also adds essential services and drivers needed to start networking.
Safe Mode with Command Prompt (Safeboot_Option=Minimal)	Similar to standard safe mode but loads the command interpreter instead of Explorer.exe as the user shell.
Enable Boot Logging	Creates a log file, Ntbtlog.txt, during startup where the names and status of all drivers loaded into memory are recorded. The log file is stored in the %SystemRoot% folder.
Enable VGA Mode	Starts the computer in basic VGA mode in cases of corruption or incompatibility of currently installed video driver. The basic video driver is always used when you start Windows 2000 in any kind of safe mode.
Last Known Good Configuration	Starts Windows 2000 using the settings (registry information) that Windows saved at the last shutdown. Use Last Known Good Configuration only in cases of incorrect configuration. It does not solve problems caused by corrupted or missing drivers or files. All system setting changes made after the last successful startup are lost.
Directory Service Restore Mode	Allows restores of Active Directory on a domain controller. This option is not available on computers that are running Windows 2000 Professional or on member servers.
Debugging Mode	Starts Windows 2000 in kernel debug mode, which allows a debugger to access the kernel for troubleshooting and system analysis.
Boot Normally	Starts Windows 2000, loading all normal startup files and registry values.

If you are using, or have used, Remote Install Services to install Windows 2000 on your computer, the advanced startup options might include options related to restoring or recovering your system using Remote Install Services, in addition to the options described above.

If you plan to start the computer in safe mode and then use Backup with Removable Storage, the only safe mode options you can use are **Enable VGA Mode**, **Last Known Good Configuration**, and **Directory Services Restore Mode**.

When the computer is started with any of the safe mode options except **Last Known Good Configuration**, a boot log of devices and services that are loading is created. The log is saved to the file Ntbtlog.txt in the folder in which Windows 2000 is installed (typically \Winnt).

If the problem was caused by a newly-installed driver, you might be able to start the computer using the **Last Known Good Configuration** option so you can research the problem with the driver. If there were other causes, after starting the computer in safe mode, you can use Event Viewer, System Information, Control Panel, Backup, and other tools to try to diagnose and correct the problem.

Recovery Console

The Recovery Console is a command-line console designed to help you recover when your Windows 2000-based computer does not start. You can use the Recovery Console after starting the computer with the Windows 2000 Setup CD or the Setup floppy disks. You can use the Recovery Console to obtain limited access to NTFS, FAT, and FAT32 volumes without starting the graphical interface.

To use the Recover Console, you must be logged on as an administrator.

Caution The Recovery Console is powerful. It is recommended that you use Recovery Console only if you are an advanced user or administrator who can use basic commands to identify and locate problem drivers and files.

Each time you use Backup to back up the system state data, a copy of the registry is placed on the local system partition in a subfolder of %SystemRoot%\Repair\RegBack. You can use the Recovery Console to copy files from %SystemRoot%\Repair\RegBack to %SystemRoot%\System32\Config (the location of the registry). After you do this, the registry contains the information it had when the system state was last backed up. Changes made after that time are lost.

Caution 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.

For more information about the Recovery Console, including a list and description of available commands, see “Repair, Recovery, and Restore” in this book.

Emergency Repair Disk

If your system does not start, and neither safe mode nor the Recovery Console has helped, you can try using the Emergency Repair Disk option in Backup. If you have prepared an ERD beforehand, you can use it to repair system files (after you start the system using the Windows 2000 Setup CD or Setup floppy disks).

The ERD can make only basic system repairs, such as to the system files, the boot sector, and the startup environment. The ERD does not back up data or programs, and it is not a replacement for regular system backups.

For more information about the ERD, see “Repair, Recovery, and Restore” in this book.

If you cannot fix the problem by using one of the options described above, try removing the disk from the computer and installing it as a second disk on another computer that is running Windows 2000. You can then use Windows 2000-based utilities for troubleshooting. For more information about using disk troubleshooting utilities, see the Windows 2000 Resource Kit Tools Help.

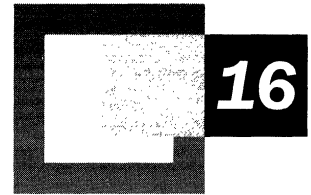
Caution Moving disks between computers is not recommended because problems can arise if the disk controllers on the two systems are incompatible or are configured differently. However, if the two computers have the same configuration, you might be able to identify and correct the problem.

Additional Resources

- For more information about troubleshooting startup problems, see the Microsoft Knowledge Base link on the Web Resources page at <http://windows.microsoft.com/windows2000/reskit/webresources>.

C H A P T E R 16

Windows 2000 Stop Messages



When Microsoft® Windows® 2000 detects an error condition from which it cannot recover, it generates a variety of system messages including Stop messages and hardware malfunction messages, commonly referred to as blue screen messages. Interpreting the meaning of various Stop messages and taking appropriate action to resolve the problems that generated the errors are critical skills in a production environment. In addition, it is vital that technical support personnel and power users know how to handle system hardware failure correctly. This chapter contains general information and troubleshooting tips about these types of errors as well as specific information about the twelve most common Stop messages seen by callers to Microsoft Product Support.

In This Chapter

System Messages 639

Stop Messages 639

Troubleshooting Stop Messages 644

Hardware Malfunction Messages 672

System Messages

The two types of system messages generated by Windows 2000 depend on the event being reported. Both are generated in character mode.

Stop messages occur when the Windows 2000 kernel detects a condition from which it cannot recover.

Hardware malfunction message occur when the processor detects a hardware condition from which the system cannot recover.

These messages were created to cover everything that might happen to halt the system, so you are unlikely to see most of them. For example, the Stop message 0x0000003E, or “Multiprocessor Configuration Not Supported” is displayed only if multiple but asymmetric central processing unit (CPU) types, such as a Pentium and a Pentium III, are installed on the same system.

To diagnose and resolve Stop messages, many users also need technical assistance from a person who has been trained to support Windows 2000. In some circumstances, running a kernel debugger on the faulty system might be required.

Stop Messages

Stop messages are always displayed on a full screen in character mode, as shown in Figure 16.1, rather than in a window. Each message is uniquely identified by a hexadecimal number and a string indicating the error's symbolic name. In addition, Stop messages are usually followed by a series of up to four additional hexadecimal numbers, shown in parentheses, which identify error parameters, as shown in the following example:

```
*** STOP: 0x0000001E (0xC0000005, 0xFDE38AF9, 0x00000001, 0x7E8B0EB4)
KMODE_EXCEPTION_NOT_HANDLED ***
```

To a trained support technician, the content of the symbolic name string might suggest which part of the system is affected by the error that left the kernel no recourse but to stop. However, it is also possible that the cause might be in another part of the system. Figure 16.1 is an example of a complete Stop message screen generated by Windows 2000.

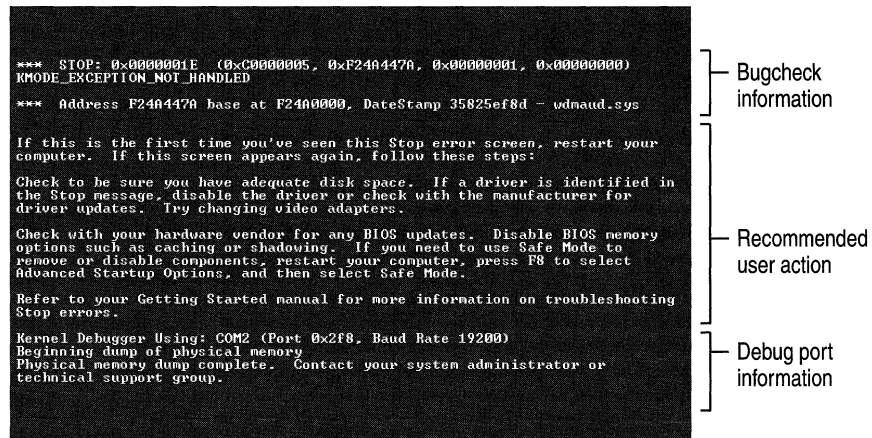


Figure 16.1 Stop Message Screen

Stop Message Screen Sections

As shown in Figure 16.1, a Windows 2000 Stop message screen contains three major sections: bugcheck information, recommended user action, and debug port information. Whenever a Stop message is displayed, first examine the bugcheck information section for assistance with troubleshooting. Second, examine the recommended user action section for troubleshooting information; Windows 2000 now incorporates troubleshooting tips, including some custom tips relevant to the particular error detected. Finally, check the debug port information section to see whether or not a memory dump file was saved for later use by a debugger.

Bugcheck Information

The bugcheck information section includes the Stop error code, also known as the bugcheck code, which contains up to four developer-defined parameters, enclosed in parentheses, and the symbolic name of the error. In Figure 16.1, the Stop error code is 0x0000001E and its symbolic name is KMODE_EXCEPTION_NOT_HANDLED.

The bugcheck information section frequently, but not always, includes a line that lists the specific hexadecimal memory address of the problem's source, along with the name of the particular driver or device in question. The type of problem detected determines whether or not this information is displayed.

Under some conditions, the kernel displays only the first line of the Stop message. This can occur if vital services needed for the display have been affected by the error.

Recommended User Action

The recommended user action section provides a list of suggestions for recovering from the error. In some cases, a simple restart might be all that is necessary because the problem is not likely to recur. In other cases, even after restarting, the Stop message returns and you are faced with getting back to an operable state. Often, this means either backing out of a recent change or, in the case of Windows 2000 setup, pinpointing and eliminating the source of the problem.

Tip A generic list of troubleshooting tips is displayed when no specific text for a Stop message exists. For some Stop messages, tips specific to the problem are listed.

Debug Port Information

The debug port information section provides confirmation of the communications parameters (COM port and bits per second data transmission rate) used by the kernel debugger on the computer, if the kernel debugger is enabled. It also indicates whether a memory dump file was saved (the dump file indicator will be displayed only if that feature is enabled).

Types of Stop Messages

Stop messages generally fall into one of four categories:

- Messages that appear during general use of Windows 2000.
- Messages that appear during the installation of Windows 2000.
- Messages that appear only during the relatively short Phase 4 period of the Windows 2000 Executive initialization sequence.
- Messages that can be traced to a software condition, called a *software trap*, detected by the processor.

General Stop Messages

The most common Stop messages are generated during regular operations. Even in a complex and robust operating system such as Windows 2000, catastrophic problems sometimes cause the system to stop responding and display a Stop message. In Windows 2000, a driver or the file system can generate a Stop message by introducing an unhandled error (exception) in the code or by performing some illegal operation.

For information about troubleshooting Stop messages, including detailed information about the most common errors, see “Troubleshooting Stop Messages” later in this chapter.

For the most comprehensive list of Stop messages in Windows 2000, along with useful information about diagnosing and troubleshooting these messages, refer to the Microsoft Knowledge Base article Q103059, titled “Descriptions of Bug Codes for Windows NT.”

Stop Messages During Installation

An unsuccessful attempt to install Windows 2000 can result in a Stop message. When this happens, first check that the computer and all of its peripheral hardware are compatible with Windows 2000. To do this, refer to the latest Windows 2000 Hardware Compatibility List (HCL). Microsoft compiles the HCL through rigorous component and compatibility testing of computers and peripheral hardware to determine if they work well with Windows 2000. For more information about the HCL, see “Additional Resources” at the end of this chapter.

If the hardware you use is not included on the Windows 2000 HCL, contact the hardware manufacturer as a first-line resource for available information, newly tested hardware, and Basic Input/Output System (BIOS) and firmware revisions. Reducing the number of hardware components by removing nonessential peripherals and devices can help you pinpoint installation conflicts as well.

Stop Messages That Occur Only at Executive Initialization

Some Stop messages occur only during the relatively short Phase 4 period of the Windows 2000 startup sequence. Initialization of the *Windows 2000 Executive*, a family of software components that provides basic operating system services, is one step during Phase 4. Executive initialization can be further broken down into two phases: Phase 0 and Phase 1. During Phase 0, interrupts are disabled and only a few Executive components, such as the hardware abstraction layer (HAL), are initialized. During Phase 1 of Executive initialization, the system is fully operational, and the Windows 2000 subcomponents go through a full initialization.

Phase 0 Initialization Stop Messages

If you receive one of the Phase 0 initialization Stop messages listed in Table 16.1, run the hardware diagnostics provided by your system manufacturer.

Note In many situations, hardware failures manifest themselves as errors that generate Stop messages. This is why troubleshooting many of the Stop messages includes running hardware diagnostics on the system.

If no hardware problems are found, reinstall Windows 2000 and try to initialize it again. If you get the same message, contact a support technician.

Table 16.1 Phase 0 Initialization Stop Messages

Message ID	Symbolic Name
0x31	PHASE0_INITIALIZATION_FAILED
0x5C	HAL_INITIALIZATION_FAILED
0x5D	HEAP_INITIALIZATION_FAILED
0x5E	OBJECT_INITIALIZATION_FAILED
0x5F	SECURITY_INITIALIZATION_FAILED
0x60	PROCESS_INITIALIZATION_FAILED

Phase 1 Initialization Stop Messages

If you receive one of the Phase 1 initialization Stop messages listed in Table 16.2, reinstall Windows 2000 and try to initialize it again. If you get the same message, contact a support technician.

Table 16.2 Phase 1 Initialization Stop Messages

Message ID	Symbolic Name
0x32	PHASE1_INITIALIZATION_FAILED
0x61	HAL1_INITIALIZATION_FAILED
0x62	OBJECT1_INITIALIZATION_FAILED
0x63	SECURITY1_INITIALIZATION_FAILED
0x64	SYMBOLIC_INITIALIZATION_FAILED
0x65	MEMORY1_INITIALIZATION_FAILED
0x66	CACHE_INITIALIZATION_FAILED
0x67	CONFIG_INITIALIZATION_FAILED
0x68	FILE_INITIALIZATION_FAILED
0x69	IO1_INITIALIZATION_FAILED
0x6A	LPC_INITIALIZATION_FAILED
0x6B	PROCESS1_INITIALIZATION_FAILED
0x6C	REFMON_INITIALIZATION_FAILED
0x6D	SESSION1_INITIALIZATION_FAILED
0x6E	SESSION2_INITIALIZATION_FAILED
0x6F	SESSION3_INITIALIZATION_FAILED
0x70	SESSION4_INITIALIZATION_FAILED
0x71	SESSION5_INITIALIZATION_FAILED

Stop Messages Caused by Software Traps

Erroneous software conditions detected by the processor, called software traps, can also generate Stop messages. A software trap occurs when a processor detects a problem with executing an instruction, which causes it to stop. For example, a processor does not carry out an instruction whose variables contains invalid data types.

When you receive one of these messages, first write down the information displayed in the bugcheck information section of the Stop message, and then restart the computer. If the message recurs, you have four options for diagnosing the Stop error, all of which should be handled by a trained support technician at your own site:

- Diagnose the problem by using the information and troubleshooting tips displayed in the Stop message. For more information see “Troubleshooting Stop Messages” later in this chapter and in the Windows 2000 Error and Event Messages Help, where message explanations and recommended user actions for the most common Stop messages are listed. This file is located on the *Microsoft® Windows® 2000 Resource Kit* companion CD.
- Contact your own or another technical support group to discuss the information in the Stop message. They might recognize a familiar pattern in the information and be able to offer assistance.

Important If you use either of the following options, be sure Windows 2000 is in debug mode before you restart your computer.

- Set up the Windows 2000 kernel debugger to gather more information about the problem.
- Contact your own or another technical support group for assistance in the remote use of the Windows 2000 kernel debugger.

Troubleshooting Stop Messages

Many problems can be resolved through troubleshooting procedures, such as verifying instructions, reinstalling key components, and verifying file dates. Also, diagnostic tools such as Winmsd, Network Monitor, and Network General Sniffer, and those found on the *Windows 2000 Resource Kit* companion CD might isolate and resolve these issues.

Generic Troubleshooting Procedures

For general troubleshooting of Windows 2000 Stop messages, follow these suggestions:

- If new hardware has been added to the system recently, remove it or replace it to see if that resolves the error. Also, try running hardware diagnostics supplied by the system manufacturer. Check with the manufacturer to see if an updated system BIOS or firmware is available. Make sure that any expansion boards are properly seated and all cables are completely connected.
- Confirm that any new hardware is listed on the Windows 2000 Hardware Compatibility List (HCL). For more information about the HCL, see “Additional Resources” at the end of this chapter.
- If new device drivers or system services have been added recently, remove them or update them to see if the problem is resolved. You need to use Safe Mode to remove or disable components, since Safe Mode loads only the minimum required drivers and system services during the startup of Windows. To enter Safe Mode, restart your computer, and press F8 at the character-mode screen that displays the prompt “For troubleshooting and advanced startup options for Windows 2000, press F8.” At the resulting Windows 2000 Advanced Options menu, choose Safe Mode. For more information about Safe Mode, see chapter “Startup Process” in this book.
- Check the computer with an up-to-date virus scanner program that is compatible with Windows 2000. Viruses can infect all types of Windows-formatted hard disks, and resulting disk corruption can generate system stop messages. Make sure the virus scanner checks the master boot record for infections.
- Verify that any recently added software is listed as compatible with Windows 2000. If it is not, check with the manufacturer to see if an update or a patch is available. Otherwise, remove the program to see if this resolves the error.
- Verify that the system has the latest Service Pack installed. To check which Service Pack, if any, is installed on your system, click **Start**, click **Run**, type **winver**, and then press ENTER. The **About Windows 2000** dialog box displays the Windows version number and the version number of the Service Pack, if one has been installed. For information about downloading the latest Service Packs, see “Additional Resources” at the end of this chapter.
- Disable BIOS memory options such as caching or shadowing.

- Check the System Log and Application Log in Event Viewer to see if any additional error messages have been logged recently. These might pinpoint the cause of the error.
- Check the Microsoft Knowledge Base link using the keywords **winnt** and the full Stop error code, such as the example in Figure 16.1, **0x0000001E**. For information about the Microsoft Knowledge Base link, see “Additional Resources” at the end of this chapter.

Kernel debugging is especially helpful when other troubleshooting techniques have failed, or when a problem repeats often. In these cases, it is possible to pinpoint the failing code in a driver or an application by using a kernel debugger. For kernel debugging, it is important to capture the exact text in the bugcheck information section of the error message. Also, in order to isolate a complex problem and develop a viable workaround or a program replacement, it is essential to record the exact steps leading to the failure.

Troubleshooting Common Stop Messages

For the most commonly encountered Stop messages, troubleshooting tips and recommendations have been gathered together to help you resolve the problem on your own. If the error persists after you have tried all of the recommendations listed both here and within the Stop message display, contact your technical support group for further assistance.

Stop 0x0000000A or IRQL_NOT_LESS_OR_EQUAL

This Stop message, also known as Stop 0xA, indicates that a kernel-mode process attempted to access a portion of memory at an Interrupt Request Level (IRQL) that was too high. A kernel-mode process can only access other processes that have an IRQL lesser than or equal to its own.

Interpreting the Message

The four parameters listed in the Stop 0xA message are defined in order of appearance as follows:

1. Memory address referenced
2. IRQL
3. Type of access (0 = read operation, 1 = write operation)
4. Address that referenced memory in parameter 1

If the third parameter is the same as the first parameter, a special condition exists in which a system worker routine, executed by a worker thread to handle background tasks known as work items, returned at a raised IRQL. In that case, the parameters are defined as follows:

1. Address of the worker routine
2. IRQL
3. Address of the worker routine
4. Address of the work item

Resolving the Problem

Buggy device driver, system service or BIOS. The error that generates Stop 0xA usually occurs after the installation of a buggy device driver, system service, or BIOS. To resolve it quickly, restart your computer, and press F8 at the character-mode screen that displays the prompt “For troubleshooting and advanced startup options for Windows 2000, press F8.” At the resulting Windows 2000 Advanced Options menu, choose the **Last Known Good Configuration** option. This option is most effective when only one driver or service is added at a time.

Incompatible device driver, system service, virus scanner or backup tool. If you encounter Stop 0xA while upgrading to a newer version of Windows, it might be caused by a device driver, a system service, a virus scanner, or a backup tool that is incompatible with the new version. If possible, remove all third-party device drivers and system services and disable any virus scanners prior to upgrading. Contact the software manufacturers to obtain updates of these tools.

For additional error messages that might help pinpoint the device or driver that is causing the error, check the System Log in Event Viewer. Disabling memory caching of the BIOS might also resolve this error. You should also run hardware diagnostics supplied by the system manufacturer, especially the memory scanner. For details on these procedures, see the owner’s manual for your computer.

If your system has small computer system interface (SCSI) adapters, contact the adapter manufacturer to obtain updated Windows 2000 drivers. Try disabling sync negotiation in the SCSI BIOS, checking the cabling and the SCSI IDs of each device, and confirming proper termination. For enhanced integrated device electronics (EIDE) devices, define the onboard EIDE port as Primary only. Also, check each EIDE device for the proper master/slave or stand-alone setting. Try removing all EIDE devices except for hard disks.

If the message appears during an installation of Windows 2000, make sure that the computer and all installed peripherals are listed on the Microsoft Windows 2000 Hardware Compatibility List (HCL). For more information about the HCL, see “Additional Resources” at the end of this chapter.

Microsoft periodically releases a package of product improvements and problem resolutions called a Service Pack. Because many problems are resolved by installing the latest Service Pack, it is recommended that all users install them as they become available. To check which Service Pack, if any, is installed on your system, click **Start**, click **Run**, type **winver**, and then press ENTER. The **About Windows 2000** dialog box displays the Windows version number and the version number of the Service Pack, if one has been installed. For information about installing the latest Service Pack, see “Additional Resources” at the end of this chapter.

Occasionally, remedies to specific problems are developed after the release of a Service Pack. These remedies are called hotfixes. Microsoft does not recommend that you install a post-Service Pack hotfix unless the specific problem it addresses has been encountered. Service Packs include all of the hotfixes released since the release of the previous Service Pack. The status of hotfix installations is not indicated in the **About Windows 2000** dialog box. For information about downloading hotfixes and Service Packs, see “Additional Resources” at the end of this chapter.

For more troubleshooting information about the 0xA Stop message, refer to the Microsoft Knowledge Base link , using the keywords **winnt** and **0x0000000A**. For information about this resource, see “Additional Resources” at the end of this chapter.

Stop 0x0000001E or KMODE_EXCEPTION_NOT_HANDLED

This Stop message, also known as Stop 0x1E, indicates that a kernel-mode process tried to execute an illegal or unknown processor instruction. This error handler is a default error handler that catches errors not associated with other specific error handlers.

Interpreting the Message

The four parameters listed in the message are defined in order of appearance as follows:

1. Exception code that was not handled
2. Address at which the exception occurred
3. Parameter 0 of the exception
4. Parameter 1 of the exception

The first parameter is a Windows 2000 error code, which is defined by the type of error encountered in the file `Ntstatus.h` of the Windows 2000 Device Driver Kit (DDK). For information about the DDK, see “Additional Resources” at the end of this chapter. The second parameter identifies the address of the module in which the error occurred. Frequently, the address points to an individual driver or piece of faulty hardware, which is generally listed on the third line of the Stop message. Always make a note of this address, as well as the link date of the driver or image that contains it. The last two parameters vary, depending upon the exception that has occurred. You can typically find a description of the parameters that are included with the name of error code in `Ntstatus.h`. If the error code has no parameters, the last two parameters are listed as `0x00000000`.

Resolving the Problem

Hardware incompatibility. First, make sure that any new hardware installed is listed on the Windows 2000 Hardware Compatibility List (HCL). For more information about the HCL, see “Additional Resources” at the end of this chapter.

Buggy device driver or system service. In addition, a buggy device driver or system service might be responsible for this error. Hardware issues, such as memory conflicts and IRQ conflicts, can also generate this error.

If a driver is listed by name within the Stop message, disable or remove that driver. Disable or remove any drivers or services that were recently added. If the error occurs during the startup sequence, restart the computer using Safe Mode to rename or delete the file. If the driver is used as part of the system startup process in Safe Mode, you need to start the computer by using the Recovery Console to access the file. For more information about Safe Mode, see chapter “Startup Process” in this book. For more information about the Recovery Console, see chapter “Repair, Recovery, and Restore” in this book.

If the problem is associated with `Win32k.sys`, the source of the error might be a third-party remote control program. If such software is installed, the service can be removed by starting the system using the Recovery Console and disabling the offending system service.

Check the System Log in Event Viewer for additional error messages that might help pinpoint the device or driver that is causing Stop `0x1E`. Disabling memory caching of the BIOS might also resolve the error. You should also run hardware diagnostics, especially the memory scanner, supplied by the system manufacturer. For details on these procedures, see the owner’s manual for your computer.

One type of this kind of error displays exception code `0x80000003`. This error indicates a hard-coded breakpoint or assertion was hit, but the system was started with the `/NODEBUG` switch. This problem should rarely occur. If it occurs repeatedly, make sure a kernel debugger is connected and the system is started with the `/DEBUG` switch.

The error that generates this message can occur after the first restart during Windows 2000 Setup, or after setup is finished. A possible cause of the error is lack of disk space for installation and system BIOS incompatibilities. For problems during Windows 2000 installation that are associated with a lack of disk space, reduce the number of files on the target hard disk. Check for and delete any unneeded temporary files, Internet cache files, application backup files, and CHK files containing saved file fragments from disk scans. You can also use another hard disk with more free space for the installation. BIOS problems can be resolved by upgrading the system BIOS version.

For more troubleshooting information about the 0x1E Stop message, refer to the Microsoft Knowledge Base link , using the keywords **winnt** and **0x0000001E**. For information about this resource, see “Additional Resources” at the end of this chapter.

Stop 0x00000024 or NTFS_FILE_SYSTEM

This Stop message, also known as Stop 0x24, indicates that a problem occurred within Ntfs.sys (the driver file that allows the system to read and write to NTFS drives).

Interpreting the Message

The four parameters listed in the message are defined in order of appearance as follows:

1. Source file and line number
2. A non-zero value contains the address of the exception record
3. A non-zero value contains the address of the context record
4. A non-zero value contains the address where the original exception occurred

All Stop messages due to problems with the file system have encoded in their first parameter the source file and the line number within the source file that generated the Stop. The high 16 bits (the first four hex digits after the 0x) identify the source file number, while the lower 16 bits (the last four hex digits of the parameter) identify the source line in the file where the stop occurred.

Resolving the Problem

Disk Corruption. Corruption in the NTFS file system or bad blocks (sectors) on the hard disk can induce this error. Corrupted SCSI and EIDE drivers can also adversely affect the system’s ability to read and write to disk, thus causing the error.

Check Event Viewer for error messages from SCSI and FASTFAT (System Log) or Autochk (Application Log) that might help pinpoint the device or driver that is causing the error. Try disabling any virus scanners, backup programs, or disk defragmenter tools that continually monitor the system. You should also run hardware diagnostics supplied by the system manufacturer. For details on these procedures, see the owner's manual for your computer. Run **Chkdsk /f /r** to detect and resolve any file system structural corruption. You must restart the system before the disk scan begins on a system partition. If you cannot start the system due to the error, use the Recovery Console and run **Chkdsk /r**. For more information about the Recovery Console, see chapter "Repair, Recovery, and Restore" in this book.

Warning If your system partition is formatted with the file allocation table (FAT16) file system, the long file names used by Windows 2000 can be damaged if Scandisk or another MS-DOS-based hard disk tool is used to verify the integrity of your hard disk from an MS-DOS prompt. (An MS-DOS prompt is typically derived from an MS-DOS startup disk or from starting MS-DOS on a multiboot system.) Always use the Windows 2000 version of Chkdsk on Windows 2000 disks.

Depletion of nonpaged pool memory. If you create a Services for Macintosh volume on a large partition (7 gigabytes or larger) with a large number of files (at least 100,000) while the AppleTalk driver Apf.sys is loaded, the indexing routine consumes a large amount of nonpaged pool memory. If the nonpaged pool memory is completely depleted, this error can stop the system. However, during the indexing process, if the amount of available nonpaged pool memory is very low, another kernel-mode driver requiring nonpaged pool memory can also trigger this error. To resolve this error, either increase the amount of installed random access memory (RAM), which increases the quantity of nonpaged pool memory available to the kernel, or reduce the number of files on the Services for Macintosh volume.

Microsoft periodically releases a package of product improvements and problem resolutions called a Service Pack. Because many problems are resolved by installing the latest Service Pack, it is recommended that all users install them as they become available. To check which Service Pack, if any, is installed on your system, click **Start**, click **Run**, type **winver**, and then press ENTER. The **About Windows 2000** dialog box displays the Windows version number and the version number of the Service Pack, if one has been installed.

Occasionally, remedies to specific problems are developed after the release of a Service Pack. These remedies are called hotfixes. Microsoft does not recommend that you install a post-Service Pack hotfix unless the specific problem it addresses has been encountered. Service Packs include all of the hotfixes released since the release of the previous Service Pack. The status of hotfix installations is not indicated in the **About Windows 2000** dialog box. For more information about Service Packs and hotfixes, see “Additional Resources” at the end of this chapter.

For more troubleshooting information about the 0x24 Stop message, refer to the Microsoft Knowledge Base link , using the keywords **winnt** and **0x00000024**. For information about this resource, see “Additional Resources” at the end of this chapter.

Stop 0x0000002E or DATA_BUS_ERROR

This message, also known as Stop 0x2E, typically indicates that a parity error in system memory has been detected. This error is almost always caused by a hardware problem—either a configuration issue, defective hardware or incompatible hardware. The exception is when a device driver has accessed an address in the 0x8xxxxxxx range that does not exist (that is, does not have a physical address mapping).

Interpreting the Message

The four parameters listed in the message are defined in order of appearance as follows:

1. Virtual address that caused the fault
2. Physical address that caused the fault
3. Processor status register (PSR)
4. Faulting instruction register (FIR)

Resolving the Problem

Hardware problem. The most common cause of this error is a hardware problem, usually related to defective RAM, Level 2 (L2) RAM cache, or video RAM.

Stop 0x2E usually occurs after the installation of faulty hardware or when existing hardware fails. If hardware has recently been added to the system, remove it to see if the error recurs. If existing hardware has failed, remove or replace the faulty component. You should run hardware diagnostics supplied by the system manufacturer to determine which hardware component has failed. For details on these procedures, see the owner's manual for your computer. Check that all the adapter cards in the computer, including memory modules, are properly seated. Use an ink eraser or an electrical contact treatment, available at electronics supply stores, to ensure adapter card contacts are clean. Be sure to wipe the cleaned contacts off, removing all cleaning debris, before reinstalling the adapter card into the computer. If compressed air is available, use it to clear out the adapter card slot.

If the problem occurs on a newly installed system, check the availability of updates for BIOS revisions on the motherboard, SCSI controllers, or network cards. Updates of this kind are typically available on the Web site or BBS of the hardware manufacturer.

If the error occurs after installing a new or updated device driver, the driver should be removed or replaced. If, under this circumstance, the error occurs during startup, restart the computer using Safe Mode to rename or delete the file. If the driver is used as part of the system startup process in Safe Mode, you need to start the computer using the Recovery Console in order to access the file. For more information about Safe Mode, see chapter "Startup Process" in this book. For more information about the Recovery Console, see chapter "Repair, Recovery, and Restore" in this book.

For additional error messages that might help pinpoint the device or driver that is causing the error, check the System Log in Event Viewer. Disabling memory caching of the BIOS might also resolve this error. In addition, check the system for viruses, using any up-to-date, commercial virus scanning software that examines the Master Boot Record of the hard disk. All Windows 2000 file systems can be infected by viruses.

Disk corruption. This error can also be a result of hard disk corruption. Run **Chkdsk /f /r** on the system partition. You must restart the system before the disk scan begins. If you cannot start the system due to the error, use the Recovery Console and run **Chkdsk /r**. For more information about the Recovery Console, see chapter “Repair, Recovery, and Restore” in this book.

Warning If your system partition is formatted with the FAT16 file system, the long file names used by Windows 2000 can be damaged if Scandisk or another MS-DOS-based hard disk tool is used to verify the integrity of your hard disk from an MS-DOS prompt. (An MS-DOS prompt is typically derived from an MS-DOS startup disk or from starting MS-DOS on a multiboot system.) Always use the Windows 2000 version of Chkdsk on Windows 2000 disks.

Microsoft periodically releases a package of product improvements and problem resolutions for Windows 2000 called a Service Pack. Because many problems are resolved by installing the latest Service Pack, it is recommended that all users install them as they become available. To check which Service Pack, if any, is installed on your system, click **Start**, click **Run**, type **winver**, and then press ENTER. The **About Windows 2000** dialog box displays the Windows version number and the version number of the Service Pack, if one has been installed.

Occasionally, remedies to specific problems are developed after the release of a Service Pack. These remedies are called hotfixes. Microsoft does not recommend that you install a post-Service Pack hotfix unless the specific problem it addresses has been encountered. Service Packs include all of the hotfixes released since the release of the previous Service Pack. The status of hotfix installations is not indicated in the **About Windows 2000** dialog box. For more information about Service Packs and hotfixes, see “Additional Resources” at the end of this chapter.

Finally, if all the above suggestions fail to resolve the error, take the system motherboard to a repair facility for diagnostic testing. A crack, a scratched trace, or a defective component on the motherboard can also cause this error.

For more troubleshooting information about the 0x2E Stop message, refer to the Microsoft Knowledge Base link , using the keywords **winnt** and **0x0000002E**. For information about this resource, see “Additional Resources” at the end of this chapter.

Stop 0x00000050 or PAGE_FAULT_IN_NONPAGED_AREA

This Stop message, also known as Stop 0x50, occurs when requested data is not found in memory. The system generates a fault, which normally indicates that the system looks for data in the paging file. In this circumstance, however, the missing data is identified as being located within an area of memory that cannot be read to disk. The system faults, but cannot find, the data and is unable to recover. Faulty hardware, a buggy system service, antivirus software, and a corrupted NTFS volume can all generate this type of error.

Interpreting the Message

The four parameters listed in the message are defined in order of appearance as follows:

1. Virtual address which caused the fault
2. Type of access (0 = read operation, 1 = write operation)
3. If not zero, the instruction address which referenced the address in parameter 1
4. Opaque information about the stop, interpreted by the kernel

Resolving the Problem

Faulty hardware. Stop 0x50 usually occurs after the installation of faulty hardware or in the event of failure of installed hardware (usually related to defective RAM, be it main memory, L2 RAM cache, or video RAM). If hardware has been added to the system recently, remove it to see if the error recurs. If existing hardware has failed, remove or replace the faulty component. You should run hardware diagnostics supplied by the system manufacturer. For details on these procedures, see the owner's manual for your computer.

Buggy system service. Often, the installation of a buggy system service is a culprit. Disable the service and confirm that this resolves the error. If so, contact the manufacturer of the system service about a possible update. If the error occurs during system startup, restart your computer, and press F8 at the character-mode screen that displays the prompt "For troubleshooting and advanced startup options for Windows 2000, press F8." At the resulting Windows 2000 Advanced Options menu, choose the **Last Known Good Configuration** option. This option is most effective when only one driver or service is added at a time.

Antivirus software. Antivirus software can also trigger this error. Disable the program and confirm that this resolves the error. If it does, contact the manufacturer of the program about a possible update.

Corrupted NTFS volume. A corrupted NTFS volume can also generate this error. Run **Chkdsk /f /r** to detect and repair disk errors. You must restart the system before the disk scan begins on a system partition. If you cannot start the system due to the error, use the Recovery Console and run **Chkdsk /r**. For more information about the Recovery Console, see chapter “Repair, Recovery, and Restore” in this book. If the hard disk is SCSI, check for problems between the SCSI controller and the disk.

Warning If your system partition is formatted with the FAT16 file system, the long file names used by Windows 2000 can be damaged if Scandisk or another MS-DOS-based hard disk tool is used to verify the integrity of your hard disk from an MS-DOS prompt. (An MS-DOS prompt is typically derived from an MS-DOS startup disk or from starting MS-DOS on a multiboot system.) Always use the Windows 2000 version of Chkdsk on Windows 2000 disks.

Finally, check the System Log in Event Viewer for additional error messages that might help pinpoint the device or driver that is causing the error. Disabling memory caching of the BIOS might also resolve this error.

Microsoft periodically releases a package of product improvements and problem resolutions for Windows 2000 called a Service Pack. Because many problems are resolved by installing the latest Service Pack, it is recommended that all users install them as they become available. To check which Service Pack, if any, is installed on your system, click **Start**, click **Run**, type **winver**, and then press ENTER. The **About Windows 2000** dialog box displays the Windows version number and the version number of the Service Pack, if one has been installed.

Occasionally, remedies to specific problems are developed after the release of a Service Pack. These remedies are called hotfixes. Microsoft does not recommend that you install a post-Service Pack hotfix unless the specific problem it addresses has been encountered. Service Packs include all of the hotfixes released since the release of the previous Service Pack. The status of hotfix installations is not indicated in the **About Windows 2000** dialog box. For more information about Service Packs and hotfixes, see “Additional Resources” at the end of this chapter.

For more troubleshooting information about the 0x50 Stop message, refer to the Microsoft Knowledge Base link , using the keywords **winnt** and **0x00000050**. For information about this resource, see “Additional Resources” at the end of this chapter.

Stop 0x00000077 or **KERNEL_STACK_INPAGE_ERROR**

This Stop message, also known as Stop 0x77, indicates that the requested page of kernel data from the paging file could not be read into memory.

Interpreting the Message

The four parameters listed in the message are defined in order of appearance as follows:

1. 0 (zero)
2. Value found in stack where signature should be
3. 0 (zero)
4. Address of signature on kernel stack

The first set of definitions apply only if the first and third parameters are both zero. Otherwise, the following definitions are applicable:

1. Status code
2. I/O status code
3. Page file number
4. Offset into page file

Frequently, the cause of this error can be determined from the second parameter, the I/O status code. Examples include:

- 0xC000009A, or STATUS_INSUFFICIENT_RESOURCES, is caused by lack of nonpaged pool resources.
- 0xC000009C, or STATUS_DEVICE_DATA_ERROR, is generally due to bad blocks (sectors) on the hard disk.
- 0xC000009D, or STATUS_DEVICE_NOT_CONNECTED, indicates defective or loose cabling, termination, or the controller not seeing the hard disk.
- 0xC000016A, or STATUS_DISK_OPERATION_FAILED, is also caused by bad blocks (sectors) on the hard disk.
- 0xC0000185, or STATUS_IO_DEVICE_ERROR, is caused by improper termination or defective cabling on SCSI devices, or two devices attempting to use the same IRQ.

These codes are the most common ones for which specific causes have been determined. For information about other possible status codes that can be returned, see the file `Ntstatus.h` of the Windows 2000 Device Driver Kit (DDK). For information about the DDK, see “Additional Resources” at the end of this chapter.

Resolving the Problem

Bad block. Stop 0x77 is caused by a bad block (sector) in a paging file or a disk controller error. In extremely rare cases, it is caused when nonpaged pool resources run out.

If the first and third parameters are zero, the stack signature in the kernel stack was not found. This error is caused by defective hardware. If the I/O status is C0000185 and the paging file is on a SCSI disk, the disk cabling and SCSI termination should be checked for problems.

Viruses. In addition, check your computer for viruses using any up-to-date, commercial virus scanning software that examines the Master Boot Record of the hard disk. All Windows 2000 file systems can be infected by viruses.

An I/O status code of 0xC000009C or 0xC000016A normally indicates that the data could not be read from the disk due to a bad block (sector). If you can restart the system after the error, Autochk runs automatically and attempts to map the bad sector to prevent its further use. If Autochk does not scan the hard disk for errors, you can manually start the disk scanner. Run **Chkdsk /f /r** on the system partition. You must restart the system before the disk scan begins. If you cannot start the system due to the error, use the Recovery Console and run **Chkdsk /r**. For more information about the Recovery Console, see chapter “Repair, Recovery, and Restore” in this book.

Warning If your system partition is formatted with the FAT16 file system, the long file names used by Windows 2000 can be damaged if Scandisk or another MS-DOS-based hard disk tool is used to verify the integrity of your hard disk from an MS-DOS prompt. (An MS-DOS prompt is typically derived from a MS-DOS startup disk or from starting MS-DOS on a multiboot system.) Always use the Windows 2000 version of Chkdsk on Windows 2000 disks.

Failing RAM. Another common cause of this error message is failing RAM. You should run hardware diagnostics supplied by the system manufacturer, especially the memory scanner. For details on these procedures, see the owner’s manual for your computer.

Also, check that all the adapter cards in the computer, including memory modules, are properly seated. Use an ink eraser or an electrical contact treatment, available at electronics supply stores, to ensure adapter card contacts are clean. Be sure to wipe the cleaned contacts off, removing all cleaning debris, before reinstalling the adapter card into the computer. If compressed air is available, use it to clear out the adapter card slot.

In addition, check the System Log in Event Viewer for additional error messages that might help pinpoint the device that is causing the error. Disabling memory caching of the BIOS might also resolve this error.

Finally, if all the above steps fail to resolve the error, take the system motherboard to a repair facility for diagnostic testing. A crack, a scratched trace, or a defective component on the motherboard can also cause this error.

For more troubleshooting information about the 0x77 Stop message, refer to the Microsoft Knowledge Base link , using the keywords **winnt** and **0x00000077**. For information about this resource, see “Additional Resources” at the end of this chapter.

Stop 0x00000079 or MISMATCHED_HAL

This message, also known as Stop 0x79, is displayed when the hardware abstraction layer (HAL) and the kernel or the computer type do not match. This error most often occurs when single-processor and multiprocessor configuration files are mixed on the same system.

Interpreting the Message

The types of mismatch parameters are defined in order of appearance in the sets as follows. The first parameter determines which set is applicable.

1. If this parameter is 1, the processor control block (PRCB) release levels mismatch (something is out of date).
2. Major PRCB level of Ntoskrnl.exe.
3. Major PRCB level of Hal.dll.
4. 0 (zero).

–Or–

1. If this parameter is 2, the build types mismatch.
2. Build type of Ntoskrnl.exe.
3. Build type of Hal.dll.
4. 0 (zero).

(Build Types: 0 = free, multiprocessor-enabled build; 1 = checked, multiprocessor-enabled build; and 2 = free, single-processor build)

Resolving the Problem

Stop 0x79 can occur if either the Ntoskrnl.exe or Hal.dll files have been manually updated. The error can also indicate that one of those two files is out of date (that is, the HAL is designed for Microsoft® Windows NT® version 4.0 and the kernel is for Windows 2000). Additionally, the computer might erroneously have a multiprocessor HAL and a single-processor kernel installed, or vice versa.

The kernel file `Ntoskrnl.exe` is for single-processor systems and `Ntkrnlmp.exe` is for multiprocessor systems. However, these file names correspond to the files on the installation media; after Windows 2000 has been installed, the file is renamed to `Ntoskrnl.exe`, regardless of the source file used. The HAL file also uses the name `Hal.dll` after installation, but there are several possible HAL files on the installation media.

To resolve this error, restart the computer using either the product CD or the four Setup disks and enter Windows 2000 Setup. Press ENTER at the “Setup Notification” screen to go to the “Welcome to Setup” screen. Press R to repair a Windows 2000 installation, and then press C to use the Recovery Console. Use the **Copy** command to copy either the correct HAL or kernel file from the original CD into the appropriate folder on the hard disk. The **Copy** command detects whether the file to be copied is in the Microsoft compressed file format. If so, it automatically expands the file copied on the target drive, although you will need to specify the correct filename extension as part of the command. These files can also be located within the `Driver.cab` file. If so, use the **Expand** command to extract them from the CAB and copy them to the hard disk. For more information about the Recovery Console, see chapter “Repair, Recovery, and Restore” in this book.

For more troubleshooting information about the 0x79 Stop message, refer to the Microsoft Knowledge Base link , using the keywords **winnt** and **0x00000079**. For information about this resource, see chapters under “Additional Resources” at the end of this chapter.

Stop 0x0000007A or KERNEL_DATA_INPAGE_ERROR

This Stop message, also known as Stop 0x7A, indicates that the requested page of kernel data from the paging file could not be read into memory.

Interpreting the Message

The four parameters listed in the message are defined in order of appearance as follows:

1. Lock type that was held (value 1, 2, 3, or Page Table Entry [PTE] address).
2. I/O status code.
3. Current process (virtual address for lock type 3, or PTE).
4. Virtual address that could not be read into memory.

For information about all possible status codes that might be returned, see the file `Ntstatus.h` of the Windows 2000 Device Driver Kit (DDK). For information about the DDK, see “Additional Resources” at the end of this chapter.

Resolving the Problem

Stop 0x7A is usually caused by a bad block (sector) in a paging file, a virus, a disk controller error, or failing RAM. In rare cases, it is caused when nonpaged pool resources run out. It is also caused by defective hardware.

SCSI problems. If the I/O status is C0000185 and the paging file is on a SCSI disk, check the disk cabling and SCSI termination for problems.

Viruses. Check your computer for viruses, using any up-to-date, commercial virus scanning software that examines the Master Boot Record of the hard disk. Any Windows 2000 file system can be infected by viruses.

Bad block. An I/O status code of 0xC000009C or 0xC000016A normally indicates the data cannot be read from the disk due to a bad block (sector). If you can restart the system after the error, Autochk runs automatically and attempts to map out the bad sector. If Autochk does not scan the hard disk for errors, you can manually launch the disk scanner. Run **Chkdsk /f /r** on the system partition. You must restart the system before the disk scan begins. If you cannot start the system due to the error, use the Recovery Console and run **Chkdsk /r**. For more information about the Recovery Console, see chapter “Repair, Recovery, and Restore” in this book.

Warning If your system partition is formatted with the FAT16 file system, the long file names used by Windows 2000 can be damaged if Scandisk or another MS-DOS-based hard disk tool is used to verify the integrity of your hard disk from an MS-DOS prompt. (An MS-DOS prompt is typically derived from a MS-DOS startup disk or from starting MS-DOS on a multiboot system.) Always use the Windows 2000 version of Chkdsk on Windows 2000 disks.

Failing RAM. Another common cause of this error message is failing RAM. Run hardware diagnostics supplied by the system manufacturer, especially the memory scanner. For details on these procedures, see the owner’s manual for your computer.

Also, check that all the adapter cards in the computer, including memory modules, are properly seated. Use an ink eraser or an electrical contact treatment, available at electronics supply stores, to ensure adapter card contacts are clean. Be sure to wipe the cleaned contacts off, removing all cleaning debris, before reinstalling the adapter card into the computer. If compressed air is available, use it to clear out the adapter card slot.

Check the System Log in Event Viewer for additional error messages that might help pinpoint the device that is causing the error. Disabling memory caching of the BIOS might also resolve it.

Microsoft periodically releases a package of product improvements and problem resolutions for Windows 2000 called a Service Pack. Because many problems are resolved by installing the latest Service Pack, it is recommended that all users install them as they become available. To check which Service Pack, if any, is installed on your system, click **Start**, click **Run**, type **winver**, and then press ENTER. The **About Windows 2000** dialog box displays the Windows version number and the version number of the Service Pack, if one has been installed.

Occasionally, remedies to specific problems are developed after the release of a Service Pack. These remedies are called hotfixes. Microsoft does not recommend that you install a post-Service Pack hotfix unless the specific problem it addresses has been encountered. Service Packs include all of the hotfixes released since the release of the previous Service Pack. The status of hotfix installations is not indicated in the **About Windows 2000** dialog box. For more information about Service Packs and hotfixes, see “Additional Resources” at the end of this chapter.

Finally, if all the above steps fail to resolve the error, take the system motherboard to a repair facility for diagnostic testing. A crack, a scratched trace, or a defective component on the motherboard can also cause this error.

For more troubleshooting information about the 0x7A Stop message, refer to the Microsoft Knowledge Base link , using the keywords **winnt** and **0x0000007A**. For information about this resource, see “Additional Resources” at the end of this chapter.

Stop 0x0000007B or INACCESSIBLE_BOOT_DEVICE

This Stop message, also known as Stop 0x7B, indicates that Windows 2000 lost access to the system partition during the startup process. This error always occurs while the system is starting and cannot be debugged because it generally occurs before the operating system has loaded the debugger.

Interpreting the Message

The four parameters listed in the message are defined in order of appearance as follows:

1. Address of a Unicode string data structure representing the Advanced RISC Computing (ARC) specification name of the device from which the startup was being attempted
2. Pointer to ARC name string in memory
3. 0 (zero)
4. 0 (zero)

The first parameter typically contains two separate pieces of data. For example, if the parameter is 0x00800020, 0x0020 is the actual length of the Unicode string and 0x0080 is the maximum name string length. The next parameter contains the address of the buffer. This address is in system space, so the high-order bit is set.

If the file system that is supposed to read the boot device failed to initialize or simply did not recognize the data on the boot device as a file system structure, the following parameter definition applies:

1. Address of the device object that could not be mounted
2. 0 (zero)
3. 0 (zero)
4. 0 (zero)

The value of the first argument determines whether the argument is a pointer to an ARC name string (ARC names are a generic method of identifying devices within the ARC environment) or a device object, because a Unicode string never has an odd number of bytes, and a device object always has a Type code of 0003.

Resolving the Problem

Failed boot device. During I/O system initialization, the boot device driver might have failed to initialize the boot device (typically a hard disk). File system initialization might have failed because it did not recognize the data on the boot device.

Also, repartitioning the system partition or installing a new SCSI adapter or disk controller might induce this error. If this happens, the Boot.ini file must be edited. For additional information about the Boot.ini file, see “Additional Resources” at the end of this chapter.

Incompatible disk hardware. If the error occurred at the initial setup of the system, the system might have been installed on an unsupported disk or SCSI controller. Some controllers are supported only by drivers that are in the Windows Driver Library (WDL), which requires the user to use a custom driver during installation. If upgrading the computer to Windows 2000, you might see a prompt to press F6 to use a custom driver. If doing a clean installation of Windows 2000, press F6 when the message “Setup is inspecting your computer’s hardware configuration...” is displayed. You will be prompted later for the new driver. If Setup autodetected the controller, you might need to skip detection and use a specific manufacturer’s diskette to load the driver. Also, check the availability of updates for the system BIOS and SCSI controller firmware. Updates of this kind are typically available on the Web site or BBS of the hardware manufacturer.

Remove any recently added hardware, especially hard disks or controllers, to see if the error is resolved. If the offending piece of hardware was a hard disk, the disk firmware version might be incompatible with Windows 2000. Contact the manufacturer for updates. If the removal of another piece of hardware resolved the error, IRQ or I/O port conflicts likely exist. Reconfigure the new device according to the manufacturer's instructions.

Confirm that all hard disks, hard disk controllers, and SCSI adapters are listed on the Microsoft Windows 2000 Hardware Compatibility List (HCL). For more information about the HCL, see "Additional Resources" at the end of this chapter.

If a driver was recently added, restart your computer, and press F8 at the character-mode screen that displays the prompt "For troubleshooting and advanced startup options for Windows 2000, press F8." At the resulting Windows 2000 Advanced Options menu, choose the **Last Known Good Configuration** option. This option is most effective when only one driver or service is added at a time.

In addition, check your computer for viruses using any up-to-date, commercial virus scanning software that examines the Master Boot Record of the hard disk. All Windows 2000 file systems can be infected by viruses.

This error can also be a result of hard disk corruption. Run **Chkdsk /f /r** on the system partition. You must restart the system before the disk scan begins. If you cannot start the system due to the error, use the Recovery Console and run **Chkdsk /r**. For more information about the Recovery Console, see chapter "Repair, Recovery, and Restore" in this book.

Warning If your system partition is formatted with the FAT16 file system, the long file names used by Windows 2000 can be damaged if Scandisk or another MS-DOS-based hard disk tool is used to verify the integrity of your hard disk from an MS-DOS prompt. (An MS-DOS prompt is typically derived from a MS-DOS startup disk or from starting MS-DOS on a multiboot system.) Always use the Windows 2000 version of Chkdsk on Windows 2000 disks.

If your system has SCSI adapters, contact the adapter manufacturer to obtain updated Windows 2000 drivers. Try disabling sync negotiation in the SCSI BIOS, checking the cabling and the SCSI IDs of each device, and confirming proper termination. For EIDE devices, define the onboard EIDE port as Primary only. Also check each EIDE device for the proper master/slave/stand alone setting. Try removing all EIDE devices except for hard disks.

For more troubleshooting information about the 0x7B Stop message, refer to the Microsoft Knowledge Base link , using the keywords **winnt** and **0x0000007B**. For information about this resource, see "Additional Resources" at the end of this chapter.

Stop 0x0000007F or UNEXPECTED_KERNEL_MODE_TRAP

This Stop message, also known as Stop 0x7F, means that one of two types of problems occurred in kernel-mode, either a kind of condition that the kernel is not allowed to have or catch (a *bound trap*), or a kind of error that is always fatal. Occasionally, this message can be caused by software problems, but the most common cause is hardware failure.

Interpreting the Message

The four parameters listed in the message are defined in order of appearance as follows:

1. Processor exception code
2. 0 (zero)
3. 0 (zero)
4. 0 (zero)

The first and most important parameter (0x0000000x) can have several different values. The cause of this error can vary, depending on the value of this parameter. All conditions that cause a Stop 0x7F can be found in any *x86* microprocessor reference manual because they are specific to the *x86* platform. Here are some of the most common exception codes:

- 0x00000000, or Divide by Zero Error, is caused when a DIV instruction is run and the divisor is 0. Memory corruption, other hardware problems, or software failures can cause this error.
- 0x00000004, or Overflow, occurs when the processor executes a call to an interrupt handler when the overflow (OF) flag is set.
- 0x00000005, or Bounds Check Fault, is generated when the processor, while executing a BOUND instruction, finds that a variable's assigned value exceeds the specified limits. A BOUND instruction is used to ensure that a signed array index is within a certain range.
- 0x00000006, or Invalid Opcode, is generated when the processor attempts to run an invalid instruction. This is generally caused when the instruction pointer has become corrupted and is pointing to the wrong location. The most common cause of this is hardware memory corruption.
- 0x00000008, or Double Fault, is when an exception occurs while trying to call the handler for a prior exception. Normally, the two exceptions can be handled serially. However, there are several exceptions that cannot be handled serially, and in this situation the processor signals a double fault. This is almost always caused by hardware problems.

Other exception codes are defined as follows:

- 0x00000001—A system-debugger call.
- 0x00000003—A debugger breakpoint.
- 0x00000007—A hardware coprocessor instruction with no coprocessor present.
- 0x0000000A—A corrupted Task State Segment.
- 0x0000000B—An access to a memory segment that was not present.
- 0x0000000C—An access to memory beyond the limits of a stack.
- 0x0000000D—An exception not covered by some other exception; a protection fault that pertains to access violations for applications.

Resolving the Problem

Hardware failure or incompatibility. Stop 0x7F usually occurs after the installation of faulty or mismatched hardware (especially memory) or in the event that installed hardware fails. If hardware was recently added to the system, remove it to see if the error recurs. If existing hardware has failed, remove or replace the faulty component. Run hardware diagnostics supplied by the system manufacturer, especially the memory scanner, to determine which hardware component has failed. For details on these procedures, see the owner's manual for your computer. Check that all the adapter cards in the computer, including memory modules, are properly seated. Use an ink eraser or an electrical contact treatment, available at electronics supply stores, to ensure adapter card contacts are clean. Be sure to wipe the cleaned contacts off, removing all cleaning debris, before reinstalling the adapter card into the computer. If compressed air is available, use it to clear out the adapter card slot.

If the error appears on a newly installed system, check the availability of updates for BIOS revisions on the motherboard, SCSI controllers, or network cards. Updates of this kind are typically available on the Web site or BBS of the hardware manufacturer.

Confirm that all hard disks, hard disk controllers, and SCSI adapters are listed on the Windows 2000 Hardware Compatibility List (HCL). For more information about the HCL, see “Additional Resources” at the end of this chapter.

If the error occurred after the installation of a new or updated device driver, the driver should be removed or replaced. If, under this circumstance, the error occurs during the startup sequence, restart the computer using Safe Mode to rename or delete the file. If the driver is used as part of the system startup process in Safe Mode, you need to start the computer using the Recovery Console in order to access the file. For more information about Safe Mode, see chapter “Startup Process” in this book. For more information about the Recovery Console, see chapter “Repair, Recovery, and Restore” in this book.

Also try restarting your computer, and press F8 at the character-mode screen that displays the prompt “For troubleshooting and advanced startup options for Windows 2000, press F8.” At the resulting Windows 2000 Advanced Options menu, choose the **Last Known Good Configuration** option. This option is most effective when only one driver or service is added at a time.

Overclocking. Setting the CPU to run at speeds above the rated specification (known as *overclocking* the CPU) can cause this error. If this has been done to the computer experiencing the error, return the CPU to the default clock speed setting.

Check the System Log in Event Viewer for additional error messages that might help pinpoint the device or driver that is causing the error. Disabling memory caching of the BIOS might also resolve it.

If you encountered this error while upgrading to Windows 2000, it might be caused by a device driver, a system service, a virus scanner, or a backup tool that is incompatible with the new version. If possible, remove all third-party device drivers and system services and disable any virus scanners prior to upgrading. Contact the software manufacturer to obtain updates of these tools.

Microsoft periodically releases a package of product improvements and problem resolutions for Windows 2000 called a Service Pack. Because many problems are resolved by installing the latest Service Pack, it is recommended that all users install them as they become available. To check which Service Pack, if any, is installed on your system, click **Start**, click **Run**, type **winver**, and then press ENTER. The **About Windows 2000** dialog box displays the Windows version number and the version number of the Service Pack, if one has been installed.

Occasionally, remedies to specific problems are developed after the release of a Service Pack. These remedies are called hotfixes. Microsoft does not recommend that you install a post-Service Pack hotfix unless the specific problem it addresses has been encountered. Service Packs include all of the hotfixes released since the release of the previous Service Pack. The status of hotfix installations is not indicated in the **About Windows 2000** dialog box. For more information about Service Packs and hotfixes, see “Additional Resources” at the end of this chapter.

Finally, if all the above steps fail to resolve the error, take the system motherboard to a repair facility for diagnostic testing. A crack, a scratched trace, or a defective component on the motherboard can also cause this error.

For more troubleshooting information about the 0x7F Stop message, refer to the Microsoft Knowledge Base link , using the keywords **winnt** and **0x0000007F**. For information about this resource, see “Additional Resources” at the end of this chapter.

Stop 0xC000021A or STATUS_SYSTEM_PROCESS_TERMINATED

This Stop message occurs when a user-mode subsystem, such as Winlogon or the Client Server Runtime Subsystem (CSRSS), is fatally compromised and security can no longer be guaranteed. The operating system switches into kernel-mode and generates this error. Because Windows 2000 cannot run without Winlogon or CSRSS, this is one of the few situations where the failure of a user-mode service can bring down the system. Running the kernel debugger is not useful in this situation because the actual error occurred in a user-mode process.

Interpreting the Message

The first three parameters listed in the message are defined in order of appearance as follows:

1. Status code
2. 0 (zero)
3. 0 (zero)

For information about all possible status codes that might be returned, see the file Ntstatus.h of the Windows 2000 Device Driver Kit (DDK). For information about the DDK, see “Additional Resources” at the end of this chapter.

Resolving the Problem

Device drivers, system services, and third-party applications. Because Stop 0xC000021A occurs in a user-mode process, the most common culprits are third-party applications. If the error occurred after the installation of a new or updated device driver, system service or third-party application, the new software should be removed or disabled. Contact the manufacturer of the software about a possible update.

If the error occurs during system startup, restart your computer, and press F8 at the character-mode screen that displays the prompt “For troubleshooting and advanced startup options for Windows 2000, press F8.” At the resulting Windows 2000 Advanced Options menu, choose the **Last Known Good Configuration** option. This option is most effective when only one driver or service is added at a time. If this does not resolve the error, try manually removing the offending software by restarting the computer in Safe Mode and renaming or uninstalling the faulty software. If the faulty software is used as part of the system startup process in Safe Mode, you need to start the computer using the Recovery Console in order to access the file. For more information about Safe Mode, see chapter “Startup Process” in this book. For more information about the Recovery Console, see chapter “Repair, Recovery, and Restore” in this book. If a newly installed piece of hardware is suspected, remove it to see if this resolves the issue.

Try running the Emergency Recovery Disk (ERD) and allow the system to repair any errors that it detects. For more information about the ERD, see chapter “Repair, Recovery, and Restore” in this book.

Mismatched system files. Mismatched system files can also cause this error. If you can successfully start the computer using Safe Mode, try using the System File Checker (SFC) to correct the problem. Open up the Run dialog box, type **sfc /scannow** and press ENTER. If SFC does not correct the problem, try running a full system restore from tape might generate this error (some restore programs might skip restoring system files they determine are in use). Check if there is an updated version of the Backup/Restore program available from the manufacturer.

Microsoft periodically releases a package of product improvements and problem resolutions for Windows 2000 called a Service Pack. Because many problems are resolved by installing the latest Service Pack, it is recommended that all users install them as they become available. To check which Service Pack, if any, is installed on your system, click **Start**, click **Run**, type **winver**, and then press ENTER. The **About Windows 2000** dialog box displays the Windows version number and the version number of the Service Pack, if one has been installed.

Occasionally, remedies to specific problems are developed after the release of a Service Pack. These remedies are called hotfixes. Microsoft does not recommend that you install a post-Service Pack hotfix unless the specific problem it addresses has been encountered. Service Packs include all of the hotfixes released since the release of the previous Service Pack. The status of hotfix installations is not indicated in the **About Windows 2000** dialog box. For more information about Service Packs and hotfixes, see “Additional Resources” at the end of this chapter.

For more troubleshooting information about the 0xC000021A Stop message, refer to the Microsoft Knowledge Base link , using the keywords **winnt** and **0xC000021A**. For information about this resource, see “Additional Resources” at the end of this chapter.

Stop 0xC0000221 or STATUS_IMAGE_CHECKSUM_MISMATCH

This Stop message indicates that a driver or a system DLL has been corrupted. Typically, the name of the damaged file is displayed as part of the message.

Resolving the Problem

To resolve this error, restart the computer using either the product CD or the four Setup disks and enter Windows 2000 Setup. Press ENTER at the “Setup Notification” screen to go to the “Welcome to Setup” screen. Press R to repair a Windows 2000 installation, then press R to start the Emergency Repair Process, and then press F to run the Fast Repair option. You will be prompted for the Emergency Recovery Disk (ERD). Allow the system to repair or replace the missing or damaged driver file on the system partition. For more information about the ERD, see chapter “Repair, Recovery, and Restore” in this book.

If you can successfully start the computer using Safe Mode, try using the System File Checker (SFC) to correct the problem. Open up the Run dialog box, type `sfc /scannow` and press ENTER.

If a specific file was identified in the Stop message as being corrupted, you can try replacing that individual file manually. Restart the system, then press F8 at the character-mode screen that displays the prompt “For troubleshooting and advanced startup options for Windows 2000, press F8.” At the resulting Windows 2000 Advanced Options menu, choose Safe Mode with Command Prompt. From there, copy a fresh version of the file from the original source onto the hard disk. If the file is used as part of the system startup process in Safe Mode, you need to start the computer using the Recovery Console in order to access the file. For more information about Safe Mode, see chapter “Startup Process” in this book. For more information about the Recovery Console, see chapter “Repair, Recovery, and Restore” in this book. If these methods fail, try reinstalling Windows 2000 and then restoring the system from a backup.

Note Some files are located in the Driver.cab located on either on the product CD or in the %SystemRoot%\Driver cache\i386 folder. Files inside the CAB file need to be extracted before they can be used. If you can successfully start the computer with Safe Mode, they can be extracted by double-clicking the CAB file in Explorer and copying the files to the target location. If you cannot start the computer, use the Recovery Console. Use the **Expand** command to extract them from the CAB and copy them to the hard disk. If the original file from the product CD is not in a CAB file but has a file name extension ending in an underscore, the file needs to be uncompressed before it can be used. The Recovery Console’s **Copy** command automatically detects compressed files and expands them as they are copied to the target location, although you will need to specify the correct filename extension as part of the command. For more information about the Recovery Console, see chapter “Repair, Recovery, and Restore” in this book..

Disk errors can be a source of file corruption. Run **Chkdsk /f /r** to detect and resolve any file system structural corruption. You must restart the system before the disk scan begins on a system partition. If you cannot start the system due to the error, use the Recovery Console and run **Chkdsk /r**. For more information about the Recovery Console, see chapter “Repair, Recovery, and Restore” in this book.

Warning If your system partition is formatted with the FAT16 file system, the long file names used by Windows 2000 can be damaged if Scandisk or another MS-DOS-based hard disk tool is used to verify the integrity of your hard disk from an MS-DOS prompt. (An MS-DOS prompt is typically derived from an MS-DOS startup disk or from starting MS-DOS on a multiboot system.) Always use the Windows 2000 version of Chkdsk on Windows 2000 disks.

If the error occurred immediately after RAM was added to the system, the paging file might be corrupted or the new RAM itself might be either faulty or incompatible.

► **To determine if newly added RAM is causing a Stop message**

1. Return the system to the original RAM configuration.
2. Use the Recovery Console to access the partition containing the paging file and delete the file Pagefile.sys. For more information about the Recovery Console, see chapter “Repair, Recovery, and Restore” in this book.
3. While still in the Recovery Console, run **Chkdsk /r** on the partition that contained the paging file.
4. Restart the system.
5. Set the paging file to an optimal level for the amount of RAM added.
6. Shut down the system and add your RAM.

The new RAM must meet the system manufacturer’s specifications for speed, parity, and type (that is, fast page mode [FPM] vs. extended data out [EDO] vs. synchronous dynamic random access memory [SDRAM]). Try to match the new RAM to the existing installed RAM as closely as possible. RAM can come in many different capacities, and more importantly, in different formats (single inline memory modules [SIMMs] or dual inline memory modules [DIMMs]). The electrical contacts can be either gold or tin and it is not wise to mix these contact types.

If you experience the same error message after reinstalling the new RAM, run hardware diagnostics supplied by the system manufacturer, especially the memory scanner. For details on these procedures, see the owner’s manual for your computer.

When you can log on to the system again, check the System Log in Event Viewer for additional error messages that might help pinpoint the device or driver that is causing the error. Disabling memory caching of the BIOS might also resolve this error.

For more troubleshooting information about the 0xC0000221 Stop message, refer to the Microsoft Knowledge Base link , using the keywords **winnt** and **0xC0000221**. For information about these resources, see “Additional Resources” at the end of this chapter.

Hardware Malfunction Messages

Hardware malfunction messages are another form of Stop messages. Like Stop messages, they are character-mode messages. They are caused by a hardware condition detected by the processor. The first one or two lines of the hardware malfunction message on one computer might differ from those on a different computer, even with the same failed component, depending upon the hardware abstraction layer (HAL) that is loaded at startup. However, these lines always convey the same idea, as shown in the following example:

```
Hardware malfunction.  
Call your hardware vendor for support.
```

The installed HAL also determines how additional lines in each system’s message differ in format and content. Therefore, before doing what the hardware malfunction message recommends, contact a support technician within your own organization to run hardware diagnostics on your computer. The information provided after the first two lines in the message helps your support technician decide which hardware diagnostics to run. For example, for ISA bus computers, this information indicates whether it is a memory-parity error or a bus-data error. On EISA computers, if the hardware problem is in an adapter, the adapter slot number on the system board is displayed.

Important In many situations, hardware failures first manifest themselves as Stop errors. Software using the failing hardware can detect problems because of unexpected results before the hardware itself has been identified as faulty. This is why troubleshooting many of the Stop messages includes running hardware diagnostics on the system.

Under rare circumstances, hardware malfunction messages can be generated by software bugs—specifically driver problems. For example, if a problematic driver writes to the wrong I/O port, the actual device at the targeted port might generate a hardware malfunction message. However, most errors of this sort are detected and debugged before the software is released to the public.

If you need help from outside your organization to interpret the information on the screen, contact the hardware manufacturer for your specific brand of computer, adapter, or peripheral device.

Additional Resources

- For more information about individual Stop messages, see the Microsoft Knowledge Base link on the Web Resources page at <http://windows.microsoft.com/windows2000/reskit/webresources>.
- The Microsoft Hardware Compatibility List (HCL) is available on the *Microsoft® Windows® 2000 Resource Kit* companion CD. See the Microsoft Hardware Compatibility List on the Web Resources page at <http://windows.microsoft.com/windows2000/reskit/webresources>.
- The latest Service Packs and hotfixes for Windows 2000 are available from Microsoft Update. Click **Start** and click **Windows Update** to see a list of components, if any, that are available as downloads for your system.
- For more information about Windows 2000 status code definitions in the file `Ntstatus.h` of the Windows 2000 Device Driver Kit (DDK), see the Device Driver Kit (DDK) link on the Web Resources page at <http://windows.microsoft.com/windows2000/reskit/webresources>.

Glossary

A

access control entry (ACE) An entry in an access control list (ACL) containing a security identifier (SID) and a set of access rights. A process with a matching security identifier is either allowed access rights, denied rights, or allowed rights with auditing.

access control list (ACL) The part of an object's security descriptor that grants or denies permission to specific users and groups to access the object. Only the owner of an object can change permissions in an ACL; thus access to the object is at the owner's discretion. See also discretionary access control list (DACL); system access control list (SACL).

ACE See access control entry.

ACL See access control list.

Active Directory The directory service included with Windows 2000 Server. It stores information about objects on a network and makes this information available to users and network administrators. Active Directory gives network users access to permitted resources anywhere on the network using a single logon process. It provides network administrators with an intuitive hierarchical view of the network and a single point of administration for all network objects. See also directory; directory service.

ActiveX A set of technologies that enables software components to interact with one another in a networked environment, regardless of the language in which the components were created.

ActiveX control A reusable software component that incorporates ActiveX technology.

ADSL See Asymmetric Digital Subscriber Line.

affinity mask A value that contains bits for each processor on the system, defining which processors a process or thread can use.

allocate To mark media for use by an application. Media in the available state may be allocated.

allocated state A state that indicates media are in use and assigned to application media pools.

AppleTalk The Apple Computer network architecture and network protocols. A network that has Macintosh clients and a computer running Windows 2000 Server with Services for Macintosh functions as an AppleTalk network.

AppleTalk Protocol The set of network protocols on which the AppleTalk network architecture is based. The AppleTalk Protocol stack must be installed on a computer running Windows 2000 Server so that Macintosh clients can connect to it. See also AppleTalk.

application media pool A data repository that determines which media can be accessed by which applications and that sets the policies for that media. There can be any number of application media pools in a Removable Storage system. Applications create application media pools.

application programming interface (API)

A set of routines that an application uses to request and carry out lower-level services performed by a computer's operating system. These routines usually carry out maintenance tasks such as managing files and displaying information.

Asymmetric Digital Subscriber Line (ADSL)

A high-bandwidth digital transmission technology that uses existing phone lines and also allows voice transmissions over the same lines. Most of the traffic is transmitted downstream to the user, generally at rates of 512 Kbps to about 6 Mbps.

attribute (object) In Active Directory, a single property of an object. An object is described by the values of its attributes. For each object class, the schema defines what attributes an instance of the class must have and what additional attributes it might have.

authoritative In the Domain Name System (DNS), the use of zones by DNS servers to register and resolve a DNS domain name. When a DNS server is configured to host a zone, it is authoritative for names within that zone. DNS servers are granted authority based on information stored in the zone.

automatic file truncation A process that converts premigrated files into a remote storage identifier or placeholder to reclaim space on the managed volume. Automatic file truncation is initiated on a managed volume whenever the amount of free space is less than the desired free space as defined by the administrator.

available state A state in which media can be allocated for use by applications.

averaging counter A type of counter that measures a value over time and displays the average of the last two measurements over some other factor (for example, PhysicalDisk\Avg. Disk Bytes/Transfer).

B

bad block A disk sector that can no longer be used for data storage, usually due to media damage or imperfections.

bar code A machine-readable label that identifies an object, such as physical media.

baseline A range of measurements derived from performance monitoring that represents acceptable performance under typical operating conditions.

basic disk A physical disk that contains primary partitions or extended partitions with logical drives used by Windows 2000 and all versions of Windows NT. Basic disks can also contain volume, striped, mirror, or RAID-5 sets that were created using Windows NT 4.0 or earlier. As long as a compatible file format is used, basic disks can be accessed by MS-DOS, Windows 95, Windows 98, and all versions of Windows NT.

basic input/output system (BIOS)

The set of essential software routines that tests hardware at startup, is involved with starting the operating system, and supports the transfer of data among hardware devices. The BIOS is stored in read-only memory (ROM) so that it can be executed when the computer is turned on. Although critical to performance, the BIOS is usually invisible to computer users.

bindery A database in Novell NetWare 2.x and 3.x that contains organizational and security information about users and groups.

BIOS See basic input/output system.

BIOS parameter block (BPB) A series of fields containing data on disk size, geometry variables, and the physical parameters of the volume. The BPB is located within the boot sector.

boot partition The volume that contains the operating system and its support files. The boot partition can be (but does not have to be) the same as the system partition. Both a primary partition and a logical drive in an extended partition can be used as a boot partition.

boot sector A critical disk structure for starting your computer located at sector 1 of each volume or floppy disk. It contains executable code and data that is required by the code, including information used by the file system to access the volume. The boot sector is created when you format the volume.

bottleneck A condition, usually involving a hardware resource, that causes the entire system to perform poorly.

bound trap In programming, a problem in which a set of conditions exceeds a permitted range of values that causes the microprocessor to stop what it is doing and handle the situation in a separate routine.

C

C2 level of security U.S. government security level that designates a system that has controls capable of enforcing access limitations on an individual basis. In a C2 system, the owner of a system resource has the right to decide who can access it, and the operating system can detect when data is accessed and by whom.

cache For DNS and WINS, a local information store of resource records for recently resolved names of remote hosts. Typically, the cache is built dynamically as the computer queries and resolves names; it helps optimize the time required to resolve queried names. See also cache file; naming service; resource record.

cache file A file used by the Domain Name System (DNS) server to preload its names cache when service is started. Also known as the “root hints” file because resource records stored in this file are used by the DNS service to help locate root servers that provide referral to authoritative servers for remote names. For Windows DNS servers, the cache file is named Cache.dns and is located in the %SystemRoot%\System32\Dns folder. See also authoritative; cache; systemroot.

caching For DNS, the ability of DNS servers to store information about the domain namespace learned during the processing and resolution of name queries. In Windows 2000, caching is also available through the DNS client service (resolver) as a way for DNS clients to keep a cache of name information learned during recent queries. See also caching resolver.

caching resolver For Windows 2000, a client-side Domain Name System (DNS) name resolution service that performs caching of recently learned DNS domain name information. The caching resolver service provides system-wide access to DNS-aware programs for resource records obtained from DNS servers during the processing of name queries. Data placed in the cache is used for a limited period of time and aged according to the active Time To Live (TTL) value. You can set the TTL either individually for each resource record (RR) or default to the minimum TTL set in the start of authority RR for the zone. See also cache; caching; expire interval; minimum TTL; resolver; resource record; Time To Live (TTL).

capture buffer The maximum size of the capture file. When the capture file reaches the maximum size, the oldest frames are removed to make room for newer frames (FIFO queue).

change journal A feature new to Windows 2000 that tracks changes to NTFS volumes, including additions, deletions, and modifications. The change journal exists on the volume as a sparse file.

changer The robotic element of an online library unit.

checkpoint In a server cluster node's registry, a snapshot of the cluster hive or of an application key; the checkpoint is written to the quorum disk when certain events take place, such as a node failure. See also cluster database; cluster hive.

child object An object that resides in another object. For example, a file is a child object that resides in a folder, which is the parent object. See also object; parent object.

Client Service for NetWare A service included with Windows 2000 Professional that allows clients to make direct connections to resources on computers running NetWare 2.x, 3.x, 4.x, or 5.x server software.

cluster database The database of configuration data (cluster objects and their settings) pertinent to the cluster. This database is the product of the cluster hive checkpoint and the changes recorded in the quorum log. A local copy of this database is maintained by all the nodes of the cluster hive in the registry. See also checkpoint; cluster hive.

cluster hive In the system registry of a server cluster node, the local copy of the cluster database; the portion of the system registry on each node that contains the configuration data of a cluster. When all the cluster nodes are up, changes to the cluster hive are synchronized on all cluster nodes, and the cluster hive is identical with the cluster database. While a node is down, that node's cluster hive is not updated with cluster configuration changes, but the changes are recorded on the quorum log. At startup, the local copy might have out-of-date information. If so, it is recreated using the last checkpoint and the change records in the quorum log. See also checkpoint; cluster database.

Cluster service Clussvc.exe, the primary executable of the Windows Clustering component that creates a server cluster, controls all aspects of its operation, and manages the cluster database. Each node in a server cluster runs one instance of the Cluster service.

COM See Component Object Model.

complementary metal-oxide semiconductor (CMOS) The battery-packed memory that stores information, such as disk types and amount of memory, used to start the computer.

completed state A state that indicates that media can no longer be used for write operations.

Component Object Model (COM) An object-based programming model designed to promote software interoperability; it allows two or more applications or components to easily cooperate with one another, even if they were written by different vendors, at different times, in different programming languages, or if they are running on different computers running different operating systems. COM is the foundation technology upon which broader technologies can be built. Object linking and embedding (OLE) technology and ActiveX are both built on top of COM.

console tree The tree view pane in a Microsoft Management Console (MMC) that displays the hierarchical namespace. By default it is the left pane of the console window, but it can be hidden. The items in the console tree (for example, Web pages, folders, and controls) and their hierarchical organization determines the management capabilities of a console. See also Microsoft Management Console (MMC); namespace.

container object An object that can logically contain other objects. For example, a folder is a container object. See also noncontainer object; object.

context switch An event that occurs when the kernel switches the processor from one thread to another, for example, when an I/O operation causes a thread to be blocked and the operating system selects another thread to run on the processor.

cyclical redundancy check (CRC)

A procedure used in checking for errors in data transmission. CRC error checking uses a complex calculation to generate a number based on the data transmitted. The sending device performs the calculation before transmission and sends its result to the receiving device. The receiving device repeats the same calculation after transmission. If both devices obtain the same result, it is assumed that the transmission was error-free. The procedure is known as a redundancy check because each transmission includes not only data but extra (redundant) error-checking values. Communications protocols such as XMODEM and Kermit use cyclical redundancy checking.

D

Data Link Control (DLC) A protocol used primarily for IBM mainframe computers and printer connectivity.

deallocate To return media to the available state after they have been used by an application.

decommissioned state A state that indicates that media have reached their allocation maximum.

deferred procedure call (DPC) A kernel-defined control object type that represents a procedure that is to be called later. A DPC runs at DISPATCH_LEVEL IRQL. A DPC can be used when a timer event occurs or when an ISR needs to perform more work but should do so at a lower interrupt request level than the one at which an ISR executes. In an SMP environment, a DPC might run immediately on a processor other than the current one, or might run after another interrupt has run on the current processor.

desired free space The amount of free space that should be maintained on a volume at all times during normal use.

device fonts Fonts that reside in your printer. They can be built into the printer itself or provided by a font cartridge or font card. See also printer fonts.

Dfs See Distributed file system.

DHCP See Dynamic Host Configuration Protocol.

direct memory access (DMA) Memory access that does not involve the microprocessor. DMA is frequently used for data transfer directly between memory and a peripheral device, such as a disk drive.

directory An information source that contains information about computer files or other objects. In a file system, a directory stores information about files. In a distributed computing environment (such as a Windows 2000 domain), the directory stores information about objects such as printers, applications, databases, and users.

directory service Both the directory information source and the service that make the information available and usable. A directory service enables the user to find an object given any one of its attributes. See also Active Directory; directory.

disconnected placeholder A placeholder whose file contents have been removed from remote storage. A disconnected placeholder could have been restored from backup after the space in remote storage was reclaimed, or the data within remote storage is physically unavailable (for example, because of a media failure).

discretionary access control list (DACL)

The part of an object's security descriptor that grants or denies specific users and groups permission to access the object. Only the owner of an object can change permissions granted or denied in a DACL; thus access to the object is at the owner's discretion. See also access control entry; object; system access control list; security descriptor.

disk bottleneck A condition that occurs when disk performance is reduced to the extent that overall system performance is affected.

disk quota The maximum amount of disk space available to a user.

Distributed file system (Dfs) A Windows 2000 service consisting of software residing on network servers and clients that transparently links shared folders located on different file servers into a single namespace for improved load sharing and data availability.

DNS server A computer that runs DNS server programs containing name-to-IP address mappings, IP address-to-name mappings, information about the domain tree structure, and other information. DNS servers also attempt to resolve client queries.

domain controller For a Windows NT Server or Windows 2000 Server domain, the server that authenticates domain logon requests and maintains the security policy and the master database for a domain. Both servers and domain controllers are capable of validating a user's logon request, but password changes must be made by contacting the domain controller.

domain local group A Windows 2000 group only available in native mode domains and can contain members from anywhere in the forest, in trusted forests, or in a trusted pre-Windows 2000 domain. Domain local groups can only grant permissions to resources within the domain in which they exist. Typically, domain local groups are used to gather security principals from across the forest to control access to resources within the domain.

dots per inch (DPI) The standard used to measure screen and printer resolution, expressed as the number of dots that a device can display or print per linear inch. The greater the number of dots per inch, the better the resolution.

DVD decoder A hardware or software component that allows a digital video disc (DVD) drive to display movies on your computer screen. See also DVD disc; DVD drive.

DVD disc A type of optical disc storage technology. A digital video disc (DVD) looks like a CD-ROM disc, but it can store greater amounts of data. DVD discs are often used to store full-length movies and other multimedia content that requires large amounts of storage space. See also DVD decoder; DVD drive.

DVD drive A disk storage device that uses digital video disc (DVD) technology. A DVD drive reads both CD-ROM and DVD discs; however, a DVD decoder is necessary to display DVD movies on your computer screen. See also DVD decoder; DVD disc.

dynamic disk A physical disk that is managed by Disk Management. Dynamic disks can contain only dynamic volumes (that is, volumes created by using Disk Management). Dynamic disks cannot contain partitions or logical drives, nor can they be accessed by MS-DOS. See also dynamic volume; partition.

Dynamic Host Configuration Protocol (DHCP)

A networking protocol that provides safe, reliable, and simple TCP/IP network configuration and offers dynamic configuration of Internet Protocol (IP) addresses for computers. DHCP ensures that address conflicts do not occur and helps conserve the use of IP addresses through centralized management of address allocation.

dynamic priority The priority value to which a thread's base priority is adjusted to optimize scheduling.

dynamic volume A logical volume that is created using Disk Management. Dynamic volumes include simple, spanned, striped, mirrored, and RAID-5 volumes. Dynamic volumes must be created on dynamic disks. See also dynamic disk; volume.

dynamic-link library (DLL) A feature of the Microsoft Windows family of operating systems and the OS/2 operating system. DLLs allow executable routines, generally serving a specific function or set of functions, to be stored separately as files with .dll extensions, and to be loaded only when needed by the program that calls them.

E

EFS See Encrypting File System.

emergency repair disk (ERD) A disk, created by the Backup utility, that contains copies of three of the files stored in the %SystemRoot%/Repair folder, including Setup.log that contains a list of system files installed on the computer. This disk can be used during the Emergency Repair Process to repair your computer if it will not start or if your system files are damaged or erased.

Encrypting File System (EFS) A Windows 2000 feature that enables users to encrypt files and folders on an NTFS volume disk to keep them safe from access by intruders. In the registry, a feature that allows the file system to automatically encrypt and decrypt file data as it is read and written to the disk, which prevents users from being able to start under MS-DOS or another operating system and then use a low-level disk editing utility to view data stored on an NTFS volume. See also NTFS file system.

Enhanced Integrated Drive Electronics (EIDE)

An extension of the IDE standard, EIDE is a hardware interface standard for disk drive designs that houses control circuits in the drives themselves. It allows for standardized interfaces to the system bus, while providing for advanced features, such as burst data transfers and direct data access.

event logging The Windows 2000 process of recording an audit entry in the audit trail whenever certain events occur, such as services starting and stopping or users logging on and off and accessing resources. You can use Event Viewer to review Services for Macintosh events as well as Windows 2000 events.

expire interval For DNS, the number of seconds that DNS servers operating as secondary masters for a zone use to determine if zone data should be expired when the zone is not refreshed and renewed.

Extended Industry Standard Architecture (EISA)

A 32-bit bus standard introduced in 1988 by a consortium of nine computer-industry companies. EISA maintains compatibility with the earlier Industry Standard Architecture (ISA) but provides for additional features.

F

failback (v., fail back) In a server cluster, the moving of a failed-over group to the next node on the group's Preferred Owners list. See also failover; node; resource.

failover (v., fail over) In a server cluster, the means of providing high availability. Upon failure, either of a resource in a group or of the node where the group is online, the cluster takes the group offline on that node, and then brings it online on another node. See also node; resource.

FAT See file allocation table.

fault tolerance The assurance of data integrity when hardware failures occur. On the Windows NT and Windows 2000 platforms, fault tolerance is provided by the Ftdisk.sys driver.

FIFO First in, first out.

file allocation table (FAT) A file system based on a file allocation table (FAT) maintained by some operating systems, including Windows NT and Windows 2000, to keep track of the status of various segments of disk space used for file storage.

file system In an operating system, the overall structure in which files are named, stored, and organized. NTFS, FAT, and FAT32 are types of file systems.

File Transfer Protocol (FTP) A protocol that defines how to transfer files from one computer to another over the Internet. FTP is also a client/server application that moves files using this protocol.

foreground boost A mechanism that increases the priority of a foreground application.

FTP See File Transfer Protocol.

G

global group For Windows 2000 Server, a group that can be used in its own domain, in member servers and in workstations of the domain, and in trusting domains. In all those places a global group can be granted rights and permissions and can become a member of local groups. However, a global group can contain user accounts only from its own domain. See also group; local group.

globally unique identifier (GUID) A 16-byte value generated from the unique identifier on a device, the current date and time, and a sequence number. A GUID is used to identify a particular device or component.

graphical user interface (GUI) A display format, like that of Windows, that represents a program's functions with graphic images such as buttons and icons. GUIs allow a user to perform operations and make choices by pointing and clicking with a mouse.

group A collection of users, computers, contacts, and other groups. Groups can be used as security or as e-mail distribution collections. Distribution groups are used only for e-mail. Security groups are used both to grant access to resources and as e-mail distribution lists. In a server cluster, a group is a collection of resources, and the basic unit of failover. See also domain local group; global group.

Group Policy An administrator's tool for defining and controlling how programs, network resources, and the operating system operate for users and computers in an organization. In an Active Directory environment, Group Policy is applied to users or computers on the basis of their membership in sites, domains, or organizational units.

H

HAL See hardware abstraction layer.

hard affinity A mechanism by which a thread can only run on a set of processors.

hardware abstraction layer (HAL)

A thin layer of software provided by the hardware manufacturer that hides, or abstracts, hardware differences from higher layers of the operating system. Through the filter provided by the HAL, different types of hardware all look alike to the rest of the operating system. This allows Windows NT and Windows 2000 to be portable from one hardware platform to another. The HAL also provides routines that allow a single device driver to support the same device on all platforms. The HAL works closely with the kernel.

Hardware Compatibility List (HCL)

A list of the devices supported by Windows 2000, available from the Microsoft Web site.

hardware malfunction message A character-based, full-screen error message displayed on a blue background. It indicates the microprocessor detected a hardware error condition from which the system cannot recover.

HCL See Hardware Compatibility List.

heartbeat In a server cluster or Network Load Balancing cluster, a periodic message sent between nodes to detect system failure of any node.

heartbeat thread A thread initiated by the Windows NT Virtual DOS Machine (NTVDM) process that interrupts every 55 milliseconds to simulate a timer interrupt.

high performance file system (HPFS)

The file system designed for the OS/2 version 1.2 operating system.

HTML See Hypertext Markup Language.

HTTP See Hypertext Transfer Protocol.

Hypertext Markup Language (HTML)

A simple markup language used to create hypertext documents that are portable from one platform to another. HTML files are simple ASCII text files with embedded codes (indicated by markup tags) to indicate formatting and hypertext links. HTML is used for formatting documents on the World Wide Web.

Hypertext Transfer Protocol (HTTP)

The protocol used to transfer information on the World Wide Web. An HTTP address (one kind of Uniform Resource Locator [URL]) takes the form: <http://www.microsoft.com>

I

ideal processor A processor associated with a thread containing a default value assigned by the system, or specified by the program developer in the application code. In Windows 2000, the scheduler favors running a thread on the ideal processor that is assigned to the thread as part of the soft affinity algorithm.

import media pool A repository where Removable Storage puts media when it recognizes the on-media identifier (OMID), but does not have the media cataloged in the current Removable Storage database.

imported state A state that indicates media whose label types are recognized by Removable Storage, but whose label IDs are not cataloged by Removable Storage.

inaccessible state A state that indicates that a side of a multi-cartridge drive is in a drive, but is not in the accessible state.

incompatible state A state that indicates that media are not compatible with the library in which they were classified. This media should be immediately ejected from the library hardware unit.

independent software vendors (ISVs)

A third-party software developer; an individual or an organization that independently creates computer software.

input/output (I/O) port A channel through which data is transferred between a device and the microprocessor. The port appears to the microprocessor as one or more memory addresses that it can use to send or receive data.

instantaneous counter A type of counter that displays the most recent measurement taken by the Performance console.

Integrated Services Digital Network (ISDN)

A type of phone line used to enhance WAN speeds. ISDN lines can transmit at speeds of 64 or 128 kilobits per second, as opposed to standard phone lines, which typically transmit at 28.8 kilobits per second. An ISDN line must be installed by the phone company at both the server site and the remote site. See also wide area network (WAN).

Internet Information Services (IIS)

Software services that support Web site creation, configuration, and management, along with other Internet functions. Internet Information Services include Network News Transfer Protocol (NNTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP). See also File Transfer Protocol (FTP); Network News Transfer Protocol (NNTP); Simple Mail Transfer Protocol (SMTP).

Internetwork Packet Exchange (IPX)

A network protocol native to NetWare that controls addressing and routing of packets within and between LANs. IPX does not guarantee that a message will be complete (no lost packets). See also Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX).

Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)

Transport protocols used in Novell NetWare and other networks.

interprocess interrupt A high Interrupt-Request Level (IRQL) interrupt that can send an interrupt from one processor to another, allowing processors to communicate.

interrupt avoidance A feature of device adapters that allows a processor to continue processing interrupts without new interrupts being queued until all pending interrupts are complete.

interrupt moderation A feature of device adapters that allows a processor to process interrupts more efficiently by grouping several interrupts to a single hardware interrupt.

interrupt request (IRQ) A signal sent by a device to get the attention of the processor when the device is ready to accept or send information. Each device sends its interrupt requests over a specific hardware line, numbered from 0 to 15. Each device must be assigned a unique IRQ number.

IP address A 32-bit address used to identify a node on an IP internetwork. Each node on the IP internetwork must be assigned a unique IP address, which is made up of the network ID, plus a unique host ID. This address is typically represented with the decimal value of each octet separated by a period (for example, 192.168.7.27). In Windows 2000, the IP address can be configured manually or dynamically through DHCP. See also Dynamic Host Configuration Protocol (DHCP); node.

ISDN See Integrated Services Digital Network.

J

job object A feature in the Win32 API set that makes it possible for groups of processes to be managed with respect to their processor usage and other factors.

K

kernel The core of layered architecture that manages the most basic operations of the operating system and the computer's processor for Windows NT and Windows 2000. The kernel schedules different blocks of executing code, called threads, for the processor to keep it as busy as possible and coordinates multiple processors to optimize performance. The kernel also synchronizes activities among Executive-level subcomponents, such as I/O Manager and Process Manager, and handles hardware exceptions and other hardware-dependent functions. The kernel works closely with the hardware abstraction layer.

L

library A data-storage system, usually managed by Removable Storage. A library consists of removable media (such as tapes or discs) and a hardware device that can read from or write to the media. There are two major types of libraries: robotic libraries (automated multiple-media, multidrive devices) and stand-alone drive libraries (manually operated, single-drive devices). A robotic library is also called a jukebox or changer. See also Removable Storage.

library request A request for an online library or stand-alone drive to perform a task. This request can be issued by an application or by Removable Storage.

Line Printer Daemon (LPD) A service on the print server that receives documents (print jobs) from line printer remote (LPR) tools running on client systems. See also Line Printer Remote (LPR).

Line Printer Remote (LPR) A connectivity tool that runs on client systems and is used to print files to a computer running an LPD server. See also Line Printer Daemon (LPD).

local area network (LAN) A communications network connecting a group of computers, printers, and other devices located within a relatively limited area (for example, a building). A LAN allows any connected device to interact with any other on the network. See also wide area network (WAN).

local group For computers running Windows 2000 Professional and member servers, a group that is granted permissions and rights from its own computer to only those resources on its own computer on which the group resides. See also global group.

local printer A printer that is directly connected to one of the ports on your computer.

local storage For Windows 2000 Server, NTFS disk volumes used as primary data storage. Such disk volumes can be managed by Remote Storage by copying infrequently accessed files to remote, or secondary, storage. See also Remote Storage.

LocalTalk The Apple networking hardware built into every Macintosh computer. LocalTalk includes the cables and connector boxes to connect components and network devices that are part of the AppleTalk network system. LocalTalk was formerly known as the AppleTalk Personal Network.

logical printer The software interface between the operating system and the printer in Windows 2000. While a printer is the device that does the actual printing, a logical printer is its software interface on the print server. This software interface determines how a print job is processed and how it is routed to its destination (to a local or network port, to a file, or to a remote print share). When a document is printed, it is spooled (or stored) on the logical printer before it is sent to the printer itself. See also spooling.

M

Master Boot Record (MBR) The data structure that starts the process of booting the computer. The most important area on a hard disk. The MBR contains the partition table for the disk and a small amount of executable code.

master file table (MFT) The database that tracks the contents of an NTFS volume. The MFT is a table whose rows correspond to files on the volume and whose columns correspond to the attributes of each file.

media access control A layer in the network architecture of Windows NT and Windows 2000 that deals with network access and collision detection.

media label library A dynamic-link library (DLL) that can interpret the format of a media label written by a Removable Storage application.

memory address A portion of computer memory that can be allocated to a device or used by a program or the operating system. Devices are usually allocated a range of memory addresses.

memory leak A condition that occurs when applications allocate memory for use but do not free allocated memory when finished.

metadata Stored data that describes and controls the functioning of the Remote Storage system.

Microsoft Management Console (MMC)

A framework for hosting administrative consoles. A console is defined by the items on its console tree, which might include folders or other containers, World Wide Web pages, and other administrative items. A console has one or more windows that can provide views of the console tree and the administrative properties, services, and events that are acted on by the items in the console tree. The main MMC window provides commands and tools for authoring consoles. The authoring features of MMC and the console tree might be hidden when a console is in User Mode. See also console tree.

migration The process of copying an object from local storage to remote storage.

minimum TTL A default Time To Live (TTL) value set in seconds for use with all resource records in a zone. This value is set in the start of authority (SOA) resource record for each zone. By default, the DNS server includes this value in query answers to inform recipients how long it can store and use resource records provided in the query answer before they must expire the stored records data. When TTL values are set for individual resource records, those values will override the minimum TTL. See also Time To Live (TTL).

mirrored volume A fault-tolerant volume that duplicates data on two physical disks. The mirror is always located on a different disk. If one of the physical disks fails, the data on the failed disk becomes unavailable, but the system continues to operate by using the unaffected disk. A mirrored volume is slower than a RAID-5 volume in read operations but faster in write operations. Mirrored volumes can only be created on dynamic disks. In Windows NT 4.0, a mirrored volume was known as a mirror set. See also dynamic disk; dynamic volume; fault tolerance; redundant array of independent disks (RAID); volume.

MMC See Microsoft Management Console.

N

namespace A set of unique names for resources or items used in a shared computing environment. The names in a namespace can be resolved to the objects they represent. For Microsoft Management Console (MMC), the namespace is represented by the console tree, which displays all of the snap-ins and resources that are accessible to a console. For Domain Name System (DNS), namespace is the vertical or hierarchical structure of the domain name tree. For example, each domain label, such as “host1” or “example,” used in a fully qualified domain name, such as “host1.example.microsoft.com,” indicates a branch in the domain namespace tree. For Active Directory, namespace corresponds to the DNS namespace in structure, but resolves Active Directory object names.

naming service A service, such as that provided by WINS or DNS, that allows friendly names to be resolved to an address or other specially defined resource data that is used to locate network resources of various types and purposes.

NetBEUI See NetBIOS Enhanced User Interface.

NetBIOS Enhanced User Interface (NetBEUI)

A network protocol native to Microsoft Networking, that is usually used in local area networks of one to 200 clients. NetBEUI uses Token Ring source routing as its only method of routing. It is the Microsoft implementation of the NetBIOS standard.

NetBIOS over TCP/IP (NetBT) A feature that provides the NetBIOS programming interface over the TCP/IP protocol. It is used for monitoring routed servers that use NetBIOS name resolution.

NetWare Core Protocol (NCP) The file-sharing protocol that governs communications about resource (such as disk and printer), bindery, and NDS operations between server and client computers on a Novell NetWare network. Requests from client computers are transmitted by the IPX protocol. Servers respond according to NCP guidelines. See also bindery; Internetwork Packet Exchange (IPX); Novell Directory Services (NDS).

network administrator A person responsible for setting up and managing domain controllers or local computers and their user and group accounts, assigning passwords and permissions, and helping users with networking issues. Administrators are members of the Administrators group and have full control over the domain or computer.

network data stream The total amount of data transferred over a network at any given time.

Network News Transfer Protocol (NNTP)

A member of the TCP/IP suite of protocols, used to distribute network news messages to NNTP servers and clients, or news-readers, on the Internet. NNTP is designed so that news articles are stored on a server in a central database, and the user selects specific items to read. See also Transmission Control Protocol/Internet Protocol (TCP/IP).

NNTP See Network News Transfer Protocol.

node In tree structures, a location on the tree that can have links to one or more items below it. In local area networks (LANs), a device that is connected to the network and is capable of communicating with other network devices. In a server cluster, a server that has Cluster service software installed and is a member of a cluster. See also local area network (LAN).

noncontainer object An object that cannot logically contain other objects. A file is a noncontainer object. See also container object; object.

Novell Directory Services (NDS) On networks running Novell NetWare 4.x and NetWare 5.x, a distributed database that maintains information about every resource on the network and provides access to these resources.

NTFS file system A recoverable file system designed for use specifically with Windows NT and Windows 2000. NTFS uses database, transaction-processing, and object paradigms to provide data security, file system reliability, and other advanced features. It supports file system recovery, large storage media, and various features for the POSIX subsystem. It also supports object-oriented applications by treating all files as objects with user-defined and system-defined attributes.

NWLink An implementation of the Internetwork Packet Exchange (IPX), Sequenced Packet Exchange (SPX), and NetBIOS protocols used in Novell networks. NWLink is a standard network protocol that supports routing and can support NetWare client/server applications, where NetWare-aware Sockets-based applications communicate with IPX/SPX Sockets-based applications. See also Internetwork Packet Exchange (IPX).

O

object An entity, such as a file, folder, shared folder, printer, or Active Directory object, described by a distinct, named set of attributes. For example, the attributes of a File object include its name, location, and size; the attributes of an Active Directory User object might include the user's first name, last name, and e-mail address. For OLE and ActiveX objects, an object can also be any piece of information that can be linked to, or embedded into, another object. See also attribute; container object; noncontainer object; parent object; child object.

object linking and embedding (OLE)

A method for sharing information among applications. Linking an object, such as a graphic, from one document to another inserts a reference to the object into the second document. Any changes you make in the object in the first document will also be made in the second document. Embedding an object inserts a copy of an object from one document into another document. Changes you make in the object in the first document will not be updated in the second unless the embedded object is explicitly updated. See also ActiveX.

offline media Media that are not connected to the computer and require external assistance to be accessed.

offset When defining a pattern match within a filter using Network Monitor, the number of bytes from the beginning of the frame where the pattern occurs in a frame.

on-media identifier (OMID) A label that is electronically recorded on each medium in a Removable Storage system. Removable Storage uses on-media identifiers to track media in the Removable Storage database. An application on-media identifier is a subset of the media label.

online library A robotic library unit, sometimes referred to as a jukebox.

operator request A request for the operator to perform a task. This request can be issued by an application or by Removable Storage.

original equipment manufacturer (OEM)

The maker of a piece of equipment. In making computers and computer-related equipment, manufacturers of original equipment typically purchase components from other manufacturers of original equipment and then integrate them into their own products.

overclocking Setting a microprocessor to run at speeds above the rated specification.

P

page-description language (PDL)

A computer language that describes the arrangement of text and graphics on a printed page. See also printer control language (PCL); PostScript.

paper source The location (such as Upper Paper Tray or Envelope Feeder) of the paper at the printer.

parent object The object in which another object resides. A parent object implies relation. For example, a folder is a parent object in which a file, or child object, resides. An object can also be both a parent and a child object. See also child object; object.

partition A logical division of a hard disk. Partitions make it easier to organize information. Each partition can be formatted for a different file system. A partition must be completely contained on one physical disk, and the partition table in the Master Boot Record for a physical disk can contain up to four entries for partitions.

pattern match In Network Monitor, specific pattern of ASCII or hexadecimal data. A pattern match can be used in setting a filter or capture trigger. See also offset.

paused The state of a node that is a fully active member in the server cluster but cannot host groups. The paused state is provided for an administrator to perform maintenance. See also; failback; failover; node.

performance counter In System Monitor, a data item associated with a performance object. For each counter selected, System Monitor presents a value corresponding to a particular aspect of the performance that is defined for the performance object. See also performance object.

Performance Monitor A Windows NT administrative tool that monitors performance on local or remote machines. Performance Monitor is replaced by the Performance console in Windows 2000. See also System Monitor.

performance object In System Monitor, a logical collection of counters that is associated with a resource or service that can be monitored. See also performance counter.

peripheral component interconnect (PCI)

A specification introduced by Intel Corporation that defines a local bus system that allows up to 10 PCI-compliant expansion cards to be installed in the computer.

physical media A storage object that data can be written to, such as a disk or magnetic tape. A physical medium is referenced by its physical media ID (PMID).

placeholder A Remote Storage identifier for an NTFS volume. See also Remote Storage.

Plug and Play A set of specifications developed by Intel that allows a computer to automatically detect and configure a device and install the appropriate device drivers.

port A mechanism that allows multiple sessions. A refinement to an IP address. In Device Manager, a connection point on a computer where devices that pass data in and out of a computer can be connected. For example, a printer is typically connected to a parallel port (also known as an LPT port), and a modem is typically connected to a serial port (also known as a COM port).

port monitor A device that controls the computer port that provides connectivity to a local or remote print device.

Portable Operating System Interface for UNIX (POSIX)

An IEEE (Institute of Electrical and Electronics Engineers) standard that defines a set of operating-system services. Programs that adhere to the POSIX standard can be easily ported from one system to another. POSIX was based on UNIX system services, but it was created in a way that allows it to be implemented by other operating systems.

POSIX See Portable Operating System Interface for UNIX.

PostScript A page-description language (PDL) developed by Adobe Systems for printing with laser printers. PostScript offers flexible font capability and high-quality graphics. It is the standard for desktop publishing because it is supported by imagesetters, the high-resolution printers used by printing services for commercial typesetting. See also printer control language (PCL); page-description language (PDL).

PostScript printer A printer that uses the PostScript page-description language (PDL) to create text and graphics on the output medium, such as paper or overhead transparency. See also page-description language (PDL); PostScript.

power-on self test (POST) A set of routines stored in read-only memory (ROM) that tests various system components such as RAM, the disk drives, and the keyboard, to see if they are properly connected and operating. If problems are found, these routines alert the user with a series of beeps or a message, often accompanied by a diagnostic numeric value. If the POST is successful, it passes control to the bootstrap loader.

premigrated file An object that has been copied to remote storage in preparation for truncation, but remains on the managed volume. When it is truncated, it will become a placeholder for the file.

print device A hardware device used for printing that is commonly called a printer. See also logical printer.

print processor A PostScript program that understands the format of a document's image file and how to print the file to a specific printer or class of printers. See also PostScript.

print server A computer that is dedicated to managing the printers on a network. The print server can be any computer on the network.

Print Server for Macintosh A Services for Macintosh service that enables Macintosh clients to send and spool documents to printers attached to a computer running Windows 2000 Server, and allows clients to send documents to printers on an AppleTalk network. Print Server for Macintosh is also called MacPrint.

print server service A service that receives print jobs from remote print clients. Different services are provided for different clients.

Print Services for UNIX A print server service for UNIX clients. See also print server service.

print spooler Software that accepts a document sent to a printer and then stores it on disk or in memory until the printer is ready for it. This collection of dynamic-link libraries (DLLs) receives, processes, schedules, and distributes documents for printing. The term spooler is an acronym created from "simultaneous print operations online." See also spooling.

printer control language (PCL) The page-description language (PDL) developed by Hewlett Packard for their laser and inkjet printers. Because of the widespread use of laser printers, this command language has become a standard in many printers. See also page-description language (PDL); PostScript.

printer driver A program designed to allow other programs to work with a particular printer without concerning themselves with the specifics of the printer's hardware and internal language. By using printer drivers that handle the subtleties of each printer, programs can communicate properly with a variety of printers. See also printer control language (PCL); PostScript.

printer fonts Fonts residing in or intended for a printer. A printer font, usually located in the printer's read-only memory (ROM), can be internal, downloaded, or on a font cartridge. See also font.

printer job language (PJL) The printer command language developed by Hewlett Packard that provides printer control at the print-job level. Using PJL commands, default printer settings such as the number of copies to print can be changed. PJL commands also permit switching printer languages between print jobs without action by the user. If bi-directional communication is supported, a PJL-compatible printer can send information such as printer model and job status to the print server. See also printer control language (PCL); page-description language (PDL); PostScript.

printer permissions Permissions that specify the type of access that a user or group has to a printer. The printer permissions are Print, Manage Printers, and Manage Documents.

printers folder The folder in Control Panel that contains the Add Printer wizard and icons for all the printers installed on your computer.

priority inversion The mechanism that allows low-priority threads to run and complete execution rather than being preempted and locking up a resource such as an I/O device.

pruning A process that removes unavailable printers from Active Directory listing. An orphan pruner program running on the domain controller periodically checks for orphaned printers, that is, printers that are offline or powered down, and deletes the printer objects of the printers it cannot find.

pull partner A Windows Internet Name Service (WINS) feature that pulls in replicas from its push partner by requesting them and then accepting the pushed replicas. See also push partner.

push partner A Windows Internet Name Service (WINS) feature that sends replicas to its pull partner upon receiving a request from the pull partner. See also pull partner.

Q

quantum A feature of a network adapter that supports its detection of all frames sent on the network.

queue A list of programs or tasks waiting for execution. In Windows 2000 printing terminology, a queue refers to a group of documents waiting to be printed. In NetWare and OS/2 environments, queues are the primary software interface between the application and print device; users submit documents to a queue. In Windows 2000, however, the printer is that interface; the document is sent to a printer, not a queue.

quorum resource A quorum-capable resource (usually a Physical Disk resource) that has been configured to manage the quorum log and cluster database checkpoints, which comprise the configuration data necessary for recovery of the cluster.

R

RAID See redundant array of independent disks.

RAID-5 volume A fault-tolerant volume with data and parity striped intermittently across three or more physical disks. Parity is a calculated value that is used to reconstruct data after a failure. If a portion of a physical disk fails, you can recreate the data that was on the failed portion from the remaining data and parity. Also known as a striped volume with parity.

recall An operation that retrieves the removed, unnamed data attribute from remote storage and places it on the managed volume. The placeholder is replaced on the managed volume with a copy of the file from remote storage. Upon completion of the recall, the file becomes a premigrated file.

redundant array of independent disks (RAID)

A method used to standardize and categorize fault-tolerant disk systems. Six levels gauge various mixes of performance, reliability, and cost. Windows 2000 provides three of the RAID levels: Level 0 (striping) which is not fault-tolerant, Level 1 (mirroring), and Level 5 (striped volume with parity). See also fault tolerance; mirrored volume; RAID-5 volume; striped volume.

registry In Windows 2000, Windows NT, Windows 98, and Windows 95, a database of information about a computer's configuration. The registry is organized in a hierarchical structure and consists of subtrees and their keys, hives, and entries.

registry key An identifier for a record or group of records in the registry.

remote procedure call (RPC) A message-passing facility that allows a distributed application to call services that are available on various machines in a network. Used during remote administration of computers.

Remote Storage A hierarchical storage management application that migrates data from primary storage to secondary storage. Hierarchical storage management makes sure that data is stored in the most cost-effective method possible. Frequently accessed data is stored on high-performance disks, while data that is not accessed as often is migrated to cheaper media until it is needed again.

remote storage For Windows 2000 Server, removable tapes in a library used for secondary data storage. Specified tapes used for secondary data storage are managed by Remote Storage and contain data that is either stored on, or has been removed from, local storage to free up disk space. See also local storage.

Removable Storage A service used for managing removable media (such as tapes and discs) and storage devices (libraries). Removable Storage allows applications to access and share the same media resources. See also library.

reparse points New NTFS file system objects that have a definable attribute containing user-controlled data and are used to extend functionality in the input/output (I/O) subsystem.

replication The process of copying data from a data store or file system to multiple computers that store the same data for the purpose of synchronizing the data. In Windows 2000, replication of Active Directory occurs through the Directory Replicator Service and replication of the file system occurs through Dfs replication.

Request for Comments (RFC) A document that defines a standard. RFCs are published by the Internet Engineering Task Force (IETF) and other working groups.

reserved state A state that indicates that a side is the second side of a two-sided medium. It is unavailable for allocation to all but the application that has already allocated the first side.

resolver DNS client programs used to look up DNS name information. Resolvers can be either a small “stub” (a limited set of programming routines that provide basic query functionality) or larger programs that provide additional lookup DNS client functions, such as caching. See also caching, caching resolver.

resource Any part of a computer system or network, such as a disk drive, printer, or memory, that can be allotted to a program or a process while it is running. For Device Manager, any of four system components that control how the devices on a computer work. These four system resources are: interrupt request (IRQ) lines, direct memory access (DMA) channels, input/output (I/O) ports, and memory addresses. In a server cluster, an instance of a resource type; the Cluster service manages various physical or logical items as resources. See also direct memory access (DMA); input/output (IO) port; interrupt request (IRQ) lines; memory address.

resource record (RR) Information in the DNS database that can be used to process client queries. Each DNS server contains the resource records it needs to answer queries for the portion of the DNS namespace for which it is authoritative.

response time The amount of time required to do work from start to finish. In a client/server environment, this is typically measured on the client side.

RFC See Request for Comments.

S

scaling The process of adding processors to a system to achieve higher throughput.

secondary storage A storage device used to store data that has been migrated from managed volumes. Secondary storage includes the part of the hard disk that is used for a migration staging area.

security descriptor A set of information attached to an object that specifies the permissions granted to users and groups, as well as the security events to be audited. See also discretionary access control list (DACL); object; system access control list (SACL).

security identifier (SID) A unique name that identifies a user who is logged on to a Windows NT or Windows 2000 security system. A security identifier can represent an individual user, a group of users, or a computer.

Server Message Block (SMB) A file-sharing protocol designed to allow networked computers to transparently access files that reside on remote systems over a variety of networks. The SMB protocol defines a series of commands that pass information between computers. SMB uses four message types: session control, file, printer, and message.

shared nothing A scalability concept in clusters and SMP systems whereby a workload is partitioned among available hardware resources. These resources are used on the workload independently, without sharing of processors, disks, or other hardware resources.

shared printer A printer that receives input from more than one computer. For example, a printer attached to another computer on the network can be shared so that it is available for many users. Also called a network printer.

Simple Mail Transfer Protocol (SMTP)

A protocol used on the Internet to transfer mail. SMTP is independent of the particular transmission subsystem and requires only a reliable, ordered, data stream channel.

Simple Network Management Protocol (SNMP)

A network management protocol installed with TCP/IP and widely used on TCP/IP and Internet Package Exchange (IPX) networks. SNMP transports management information and commands between a management program run by an administrator and the network management agent running on a host. The SNMP agent sends status information to one or more hosts when the host requests it or when a significant event occurs.

Small Computer System Interface (SCSI)

A standard high-speed parallel interface defined by the X3T9.2 committee of the American National Standards Institute (ANSI). A SCSI interface is used for connecting microcomputers to peripheral devices, such as hard disks and printers, and to other computers and local area networks.

SMTP See Simple Mail Transfer Protocol.

SNMP See Simple Network Management Protocol.

soft affinity A mechanism designed to optimize performance in a multiprocessor environment. Soft affinity favors scheduling threads on the processor in which they recently ran or the ideal processor for the thread. With soft affinity, the efficiency of the processor cache is higher because threads often run on the processor on which they previously ran. Soft affinity does not restrict a thread to run on a given processor.

software trap In programming, an event that occurs when a microprocessor detects a problem with executing an instruction, which causes it to stop.

sparse file A file that is handled in a way that requires less disk space than would otherwise be needed by allocating only meaningful non-zero data. Sparse support allows an application to create very large files without committing disk space for every byte.

spooling A process on a server in which print documents are stored on a disk until a printer is ready to process them. A spooler accepts each document from each client, stores it, and sends it to a printer when the printer is ready.

Standard TCP/IP Port Monitor A port monitor that connects a Windows 2000 print server to network-interface printers that use the TCP/IP protocol. It replaces LPRMON for TCP/IP printers connected directly to the network through a network adapter. Printers connected to a UNIX or VAX host that requires RFC 1179 compliance may still require LPRMON on the print server.

Stop error A serious error that affects the operating system and that could place data at risk. The operating system generates an obvious message, a screen with the Stop message, rather than continuing on and possibly corrupting data. Also known as a fatal system error. See also Stop message.

Stop message A character-based, full-screen error message displayed on a blue background. A Stop message indicates that the Windows 2000 kernel detected a condition from which it cannot recover. Each message is uniquely identified by a Stop error code (a hexadecimal number) and a string indicating the error's symbolic name. Stop messages are usually followed by up to four additional hexadecimal numbers, enclosed in parentheses, which identify developer-defined error parameters. A driver or device may be identified as the cause of the error. A series of troubleshooting tips are also displayed, along with an indication that, if the system was configured to do so, a memory dump file was saved for later use by a kernel debugger. See also Stop error.

storage hierarchy A directed cyclic graph of linked storage pools.

storage pool A unit of storage administered by Removable Storage and composed of homogenous storage media. A storage pool is a self-contained storage area with homogenous characteristics (for example, random access, sequential access, read/write, and write-once).

stream A sequence of bits, bytes, or other small structurally uniform units.

striped volume A volume that stores data in stripes on two or more physical disks. Data in a striped volume is allocated alternately and evenly (in stripes) to these disks. Striped volumes offer the best performance of all volumes available in Windows 2000, but they do not provide fault tolerance. If a disk in a striped volume fails, the data in the entire volume is lost. You can create striped volumes only on dynamic disks. Striped volumes cannot be mirrored or extended. In Windows NT 4.0, a striped volume was known as a stripe set. See also dynamic disk, dynamic volume, fault tolerance, volume.

symmetric interrupt distribution A mechanism for distributing interrupts across available processors.

system access control list (SACL)

The part of an object's security descriptor that specifies which events are to be audited per user or group. Examples of auditing events are file access, logon attempts, and system shutdowns. See also access control entry (ACE); discretionary access control list (DACL); object; security descriptor.

System Monitor A tool that supports detailed monitoring of the use of operating system resources. System Monitor is hosted, along with Performance Logs and Alerts, in the Performance console. The functionality of System Monitor is based on Windows NT Performance Monitor, not Windows 98 System Monitor.

System State A collection of system-specific data that can be backed up and restored. For all Windows 2000 operating systems, the System State data includes the registry, the class registration database, and the system boot files. For Windows 2000 Server, the system state data also includes the Certificate Services database (if the server is operating as a certificate server). If the server is a domain controller, the system state data also includes Active Directory and the Sysvol directory. See also Active Directory; domain controller; Sysvol.

systemroot The path and folder name where the Windows 2000 system files are located. Typically, this is C:\Winnt, although a different drive or folder can be designated when Windows 2000 is installed. The value %systemroot% can be used to replace the actual location of the folder that contains the Windows 2000 system files. To identify your systemroot folder, click Start, click Run, and then type %systemroot%.

Sysvol A shared directory that stores the server's copy of the domain's public files, which are replicated among all domain controllers in the domain. See also domain controller.

T

T1 A wide-area carrier that transmits data at 1.544 Mbps.

TCP/IP See Transmission Control Protocol/Internet Protocol.

thread A type of object within a process that runs program instructions. Using multiple threads allows concurrent operations within a process and enables one process to run different parts of its program on different processors simultaneously. A thread has its own set of registers, its own kernel stack, a thread environment block, and a user stack in the address space of its process.

thread state A numeric value indicating the execution state of the thread. Numbered 0 through 5, the states seen most often are 1 for ready, 2 for running, and 5 for waiting.

Time To Live (TTL) A timer value included in packets sent over TCP/IP-based networks that tells the recipients how long to hold or use the packet or any of its included data before expiring and discarding the packet or data. For DNS, TTL values are used in resource records within a zone to determine how long requesting clients should cache and use this information when it appears in a query response answered by a DNS server for the zone.

Token Ring A type of network media that connects clients in a closed ring and uses token passing to allow clients to use the network. See also LocalTalk.

total instance A unique instance that contains the performance counters that represent the sum of all active instances of an object.

Transmission Control Protocol/Internet Protocol (TCP/IP)

A set of software networking protocols widely used on the Internet that provide communications across interconnected networks of computers with diverse hardware architectures and operating systems. TCP/IP includes standards for how computers communicate and conventions for connecting networks and routing traffic.

TrueType fonts Fonts that are scalable and sometimes generated as bitmaps or soft fonts, depending on the capabilities of your printer. TrueType fonts are device-independent fonts that are stored as outlines. They can be sized to any height, and they can be printed exactly as they appear on the screen. See also font.

truncate To remove files that are in remote storage from local storage, reclaiming space in local storage. When a premigrated file is truncated it is converted to a remote storage identifier or placeholder.

U

UNC See Universal Naming Convention.

Unicode A fixed-width, 16-bit character-encoding standard capable of representing the letters and characters of the majority of the world's languages. Unicode was developed by a consortium of U.S. computer companies.

Uniform Resource Locator (URL)

An address that uniquely identifies a location on the Internet. A URL for a World Wide Web site is preceded with `http://`, as in the fictitious URL `http://www.example.microsoft.com/`. A URL can contain more detail, such as the name of a page of hypertext, usually identified by the file name extension `.html` or `.htm`. See also HTML; HTTP; IP address.

Universal Naming Convention (UNC)

A convention for naming files and other resources beginning with two backslashes (`\`), indicating that the resource exists on a network computer. UNC names conform to the

`\\SERVERNAME\SHARENAME` syntax, where `SERVERNAME` is the server's name and `SHARENAME` is the name of the shared resource. The UNC name of a directory or file can also include the directory path after the share name, with the following syntax:

`\\SERVERNAME\SHARENAME\DIRECTORY\FILENAME`.

Universal Serial Bus (USB) A serial bus with a bandwidth of 1.5 megabits per second (Mbps) for connecting peripherals to a microcomputer. USB can connect up to 127 peripherals, such as external CD-ROM drives, printers, modems, mice, and keyboards, to the system through a single, general-purpose port. This is accomplished by daisy chaining peripherals together. USB supports hot plugging and multiple data streams.

unnamed data attribute The default data stream of an NTFS file, sometimes referred to as `$DATA`.

unprepared state A state that indicates a side of a medium that is not claimed or used by any application, but which does not have a free label on it. Applications cannot allocate unprepared media. This is a temporary state.

unrecognized media pool A repository of blank media and media that are not recognized by Removable Storage.

unrecognized state A state that indicates that the label types and label IDs of a medium are not recognized by Removable Storage.

V

value bar The area of the System Monitor graph or histogram display that shows last, average, minimum and maximum statistics for the selected counter.

virtual memory The space on the hard disk that Windows 2000 uses as memory. Because of virtual memory, the amount of memory taken from the perspective of a process can be much greater than the actual physical memory in the computer. The operating system does this in a way that is transparent to the application, by paging data that does not fit in physical memory to and from the disk at any given instant.

volume A portion of a physical disk that functions as though it were a physically separate disk. In My Computer and Windows Explorer, volumes appear as local disks, such as drive C or drive D.

volume decommission A process that occurs when a managed volume is no longer accessible. The data in remote storage is no longer associated with a placeholder or a premigrated file. This space is available for space reclamation.

volume mount points New system objects in the version of NTFS included with Windows 2000 that represent storage volumes in a persistent, robust manner. Volume mount points allow the operating system to graft the root of a volume onto a directory.

W

WAN See wide area network.

wide area network (WAN) A communications network connecting geographically separated computers, printers, and other devices. A WAN allows any connected device to interact with any other on the network. See also local area network (LAN).

WINS database The database used to register and resolve computer names to IP addresses on Windows-based networks. The contents of this database are replicated at regular intervals throughout the network. See also push partner, pull partner, replication.

working set For a process, the amount of physical memory assigned to a process by the operating system.

Index

Symbols

12-month and 12-week schedules, backups 505 – 506
 16-bit applications
 monitoring 278 – 281
 output destination rules 192 – 193
 printing from 192
 running in separate processes 281
 24-hour schedules, backups 503
 512-byte sector maximum cluster size 17

A

Access control lists (ACLs)
 CacIs tool 152 – 153
 Removable Storage 67
 setting permissions 138 – 140
 Access is denied error message 530
 Accessing random and sequential data 391
 ACL *See* Access control lists
 Active Directory
 backing up database 512, 514
 print integration *See* Print servers; Printers
 restoring database from backup 514, 544 – 545
 Active Directory Replicator service, logon scripts 519
 Active partitions, startup disks 617
 Active sessions counter, troubleshooting Event ID 2009 411
 ActiveX control, System Monitor 282 – 288
 Activity rates, deferred procedure calls and interrupts 437
 Adapters, network *See* Network adapters
 Adapters, SCSI 43, 663
 Add counters option 239
 Add Port Wizard 195 – 196
 Add Printer Wizard 165, 178 – 179
 Add Standard TCP/IP Port Wizard 183 – 184
 Adding network adapters 427 – 428
 Address Filter item 422
 Addresses
 files, clusters as 114
 loopback, instances 399
 printer share, entering 179, 195 – 196
 Administering
 disk quotas 105 – 106
 network printing resources 217 – 219
 Removable Storage 65 – 78
 Administrative Tools menu 233
 Affinity
 hard processor 439
 soft processor 439
 sort 438
 Alerts *See* Performance Logs and Alerts
 Algorithms
 compression, NTFS 146
 hard processor 439
 soft processor 439
 sort affinity 438
 Alignment, disk 370
 Allocated state 61
 Allocation of sides in media 64
 Allow Pruning of Published Printers policy setting 208
 Allow Publishing policy setting 208
 Alternate data streams 118
 Analyzing
 disk usage *See* Performance
 memory usage *See* Memory
 processor performance *See* Processors, monitoring
 SMP system performance *See* Symmetric
 multiprocessing
 symptoms of problems 597, 599 – 600
 Antivirus programs *See* Viruses
 Apf.sys, Stop 0x24 message 651
 ApiMon (Application Monitor) 315
 AppleTalk
 drivers, Stop 0x24 message 651
 monitoring network performance 402
 printing 200 – 203
 Application layer 397
 Application log 582
 Application Monitor (ApiMon) 315

- Application pools
 - holding media with 64
 - moving tapes to 72
 - overview 56
 - Application-Layer objects counter 404 – 409
 - Applications
 - See also* Tools
 - 16-bit
 - monitoring 278 – 281
 - output destination rules 192 – 193
 - printing from 192
 - running in separate processes 281
 - antivirus *See* Viruses
 - Application Monitor (ApiMon) 315
 - backing up on local computers 519
 - bugs, hardware malfunction messages 672
 - compatibility 604
 - creating using the Job Object 329
 - design, optimizing performance 443 – 445
 - disk and cache usage 390 – 392
 - disk defragmentation 453
 - external, sharing libraries with 91
 - LeakyApp tool
 - counter activity during memory leaks 314
 - paging file usage during memory shortages 300
 - legacy, monitoring 278 – 282
 - MS-DOS, monitoring 282
 - printer drivers as 161
 - processor bottlenecks caused by 342
 - profiling 342
 - Remote Storage-aware 98 – 99
 - Removable Storage-aware 65 – 66
 - third-party
 - backup programs 546
 - remote control, Stop 0x1E message 649
 - Stop 0xC000021A message 668
 - upgrades, planning 453 – 454
 - vendor support for failures 452
 - Virtual Address Dump (Vadump) 315
 - Working Set Tuner (WST) 315
 - Application-specific media states 64
 - Archived data, backing up 519
 - Arrays, RAID 467
 - Attrib command, Recovery Console 531
 - Attribute List attribute type 126
 - Attributes
 - attribute bytes, FAT volumes 114
 - attribute definitions file 125
 - changing Boot.ini file attributes 621
 - Attributes (*continued*)
 - changing Ntdetect.com file attributes 628
 - duplicate media 59
 - files, NTFS volumes 126
 - NTFS files 85
 - reparse 150
 - Audit Object Access option 216
 - Auditing
 - disk space 107
 - printing events 214
 - spooler events 216 – 217
 - Authentication, choosing methods for printing from Internet 188 – 189
 - Auto Refresh 588
 - Autochk, Stop message 658
 - Auto-configuration, Removable Storage 69
 - Autoexec.nt 541
 - Automatic File Truncation, Remote Storage 83 – 84
 - Automatically Publish policy setting 208
 - Automating display of long and short file names 129
 - Availability of logon scripts 519
 - Available Bytes counter 257, 263
 - Available state 61
 - AVBoot tool
 - Remote Storage considerations 99
 - startup disk 37, 575
 - updating 575
 - using 37, 575
 - Averaging counters 232
 - Avg. Disk Bytes/Read counter 380
 - Avg. Disk Bytes/Transfer counter 371
 - Avg. Disk Bytes/Write counter 380
 - Avg. Disk Queue Length counter 372
 - Avg. Disk sec/Read counter 380
 - Avg. Disk sec/Transfer counter 372
 - Avg. Disk sec/Write counter 380
- ## B
- Backup Boot Sector field 29
 - Backup option, Emergency Repair Disk (ERD) 540 – 543
 - BackupPeriodicity parameter 406
 - Backups
 - applications 519
 - backup plan
 - backup strategies 496 – 498
 - example backup scenarios 501 – 505
 - guidelines 501, 507 – 510

- Backups (*continued*)
 - backup plan (*continued*)
 - scheduling backups 505 – 507
 - security considerations 498 – 501
 - testing and documenting 510
 - backup types 516
 - boot and system files 514
 - encrypted files 518
 - Exchange service 522 – 523
 - FAT volumes 139
 - local computers 497 – 498, 518, 519
 - locked files 518
 - logical volumes 523
 - logon scripts 518 – 519
 - NTFS volumes 139, 520
 - overview 515 – 516
 - placeholders 86
 - registry files 540, 515
 - remote computers 497 – 498, 520
 - Remote Storage files 520 – 522
 - Remote Storage-aware backup programs 98 – 99
 - Removable Storage databases 71 – 72
 - restoring
 - Active Directory database 514
 - Exchange 523
 - file security settings 546
 - files from backup sets 546
 - managed files 557, 557 – 558
 - placeholders 87
 - registry 544 – 545
 - system state data 512, 544 – 545
 - tapes 558 – 559
 - third-party backup programs 546
 - selecting backup media 517
 - skipped files 517 – 518
 - SQL databases 523
 - Stop 0xA message 647
 - storage devices and media types 495 – 496
 - system state data [begin] 511, 515
 - types of 495
- Backward Compatibility policy setting 208
- Bad blocks
 - hard disks 650
 - paging files 658, 661
- Bad cluster file 125
- Bad media, recovering from 558 – 559, 515 –
- Balancing network load 445 – 446
- Bar code labels, physical media 59
- Bar code readers 53
- Base file record 125
- Base priorities
 - changing, processes 358
 - monitoring 357
- Base Priority measure 252
- Baselines
 - description 381, 398
 - disk usage monitoring 381 – 384
 - memory monitoring 300 – 301
 - processor performance 330 – 331
 - setting, servers 277
 - using 261
- Basic authentication option 189
- Basic disks
 - converting to dynamic 7, 468
 - features 8, 10
 - Ftdisk tool 102
 - moving between computers 468 – 469
 - overview 5 – 6
 - partitions 7, 8
 - upgrading to dynamic 5, 7
 - volumes 5, 6
- Basic input/output system (BIOS)
 - disabling 481
 - Power-On Self Test (POST) routine 616
 - role in initial Windows 2000 startup 616
 - Stop 0x1E message 649
 - Stop message 647
- Batch command, Recovery Console 531
- Begin Logon dialog box 615
- Bi-directional printing, language monitors 176
- Binary PostScript print jobs 202
- Binding rates, TCP/IP 399
- BIOS *See* Basic input/output system
- BIOS parameter block (BPB)
 - boot sector components 24
 - description 22
 - FAT16 volumes 25 – 27
 - FAT32 volumes 29 – 31
 - NTFS volumes 31 – 33
- Bitmap attribute type 126
- Blocking Requests Rejected counter 408
- Blue screen messages 637
- Boot configurations, formatting system partitions 134
- Boot device errors 41, 663
- Boot files, backing up 514
- Boot Indicator field 14
- Boot partitions 155, 475
- Boot record *See* Master boot record

- Boot sector
 - converting from FAT to NTFS 155 – 156
 - Emergency Repair Process 543
 - location 10
 - NTFS volumes 124
 - overview 21 – 33
 - repairing damaged 38 – 41
 - viruses 35 – 38, 42
- Boot volume 7
- Boot.ini
 - /MAXMEM switch 628
 - /SOS switch 624, 628
 - bootstrap loader screen 618, 619
 - default operating system setting 619
 - editing 621 – 622
 - example 619
 - parameters 619 – 620
 - recreating using Recovery Console 540
 - sections 619
 - signature syntax 617 – 618
 - starting shadow drive from startup floppy 482
 - switches 620 – 621
- Bootstrap loader
 - choosing operating systems from 619
 - role in Windows 2000 startup 617 – 618
 - troubleshooting 626 – 627
- Bottlenecks
 - See also* Performance
 - cache 317
 - causes of 308, 309
 - counters for monitoring 259 – 260
 - disk 291, 389
 - identifying 263 – 264
 - investigating 265 – 266
 - memory 302 – 323
 - network 425 – 428
 - processor *See* Processors, bottlenecks
- Bound traps 665
- BPB *See* BIOS parameter blocks
- Bridges as cause of disrupted connections 490 – 491
- Broadcast Frames Received/second counter 400
- Browser object 227, 404 – 405
- Browser Service 405 – 406
- Browsers, viewing and managing printers 166
- B-tree structures 125
- Buffer Space Then Pattern Match trigger 420
- Buffer Space trigger 420
- Bugs, hardware malfunction messages 672
- Buttons, hiding 251

- Bytes Per Sector field 25 – 29
- Bytes Printed/sec counter 213
- Bytes Total/sec counter
 - description 407 – 408
 - monitoring network performance with 400
 - recommended threshold for 264
- Bytes Transferred/sec counter 410
- Bytes, attribute 114

C

- Cables
 - cabling disks 661
 - network, as cause of disrupted connections 490
 - troubleshooting 43
- Cache Bytes counter 257
- Cache object 227
- Caches
 - controller, deciding to enable 149
 - counters 318 – 321
 - data recovery and 149
 - evaluating effectiveness of 289 – 323
 - evaluating usage by applications 390 – 392
 - monitoring 316 – 323
- Cacsl tool 152 – 153
- Calls, deferred *See* Deferred procedure calls
- Cartridges, cleaning 75
- Case, file names 140 – 141
- Catalogs for backup and restore 558, 511
- Categorizing failures 455
- CDFS (Compact disc file system) 130
- CD-ROM
 - creating for use on Windows 2000 130
 - moving among media pools 74
 - on-media identifier handling 59
- Central processing units (CPUs)
 - avoiding failures 486
 - improving response time 332
 - monitoring processing time *See* Processes, monitoring
 - overlocking, Stop 0x7F message 667
- Centronix parallel ports 180
- Certificate Services database
 - backing up 512, 514
 - restoring from backup set 544
- Change journal
 - description 119
 - sparse stream 119
 - using in Windows NT 122, 123

- Changes in media, detecting 60
- Characterizing server workloads 275 – 277
- Chdir command, Recovery Console 532
- Check Publish State policy setting 208
- Checking hard disk integrity
 - Stop 0x77 message 658
 - Stop 0x7A message 661
 - Stop 0x7B message 664
- Checking system resources 78
- Chkdsk command, Recovery Console 532
- Classes, Priority 354 – 355
- Cleaning drives, Removable Storage 75
- Client connectivity, testing NUL port 177
- Client read, write, and memory map requests 85
- Client Service for NetWare 173, 199 – 200
- Climate control system 451
- Closing searches, MS-DOS 420
- Cls command, Recovery Console 532
- Cluster bitmap file 125
- Cluster remapping 149
- Cluster service, printing with 210 – 213
- Clusters
 - as file addresses 114
 - size
 - changing 112
 - compression limitations 141
 - decreasing 115
 - maximum 17
 - on FAT16, FAT32, and NTFS volumes 123
- CMOS, troubleshooting 42 – 43
- Collecting data, architecture for 226 – 232
- Colors property, System Monitor 240
- Colors, compressed files and folders 143
- COM + registration database
 - backing up 512, 514
- COM+ registration database
 - restoring from backups 544 – 545
- Command files, running during power failures 489
- Command line
 - changing attributes at 621
 - entering long file names 128
 - installing printers 217 – 218
- Commands, Recovery Console 531 – 538
- Commit Charge counter 257
- Commit Limit counter 257
- Committed Bytes counter 256, 257
- Compact disc file system (CDFS) 130
- Compact tool 143, 153 – 154
- Company policies, backup planning in 509
- Comparing file systems 130 – 141
- Comparison testing, preparing for 377 – 378
- Compatibility
 - applications 604
 - hardware 604
 - Remote Storage with third-party remote storage products 98
- Completed state 57, 61
- Compliance with POSIX 140 – 141
- Component Services Class Registration database
 - backing up 512, 515
 - restoring from backups 544 – 545
- Components category, System Information tool 570
- Compress tool 154 – 155
- Compressing files and folders *See* File compression
- Config.nt 541
- Configuration planning
 - avoiding single points of failure 485 – 491
 - contingency planning, system recovery 454 – 456
 - data recovery and restoration 454
 - developing system recovery plans 459 – 461
 - fault-tolerant disks 465 – 485
 - hardware and software upgrades 453 – 454
 - maintaining configuration and system information 457
 - security 453
 - system maintenance 452 – 453
 - top-down and bottom-up execution 452
 - training personnel for system recovery 462
- Configuring
 - data collection and reporting 231 – 232
 - disks and files for optimal performance 367 – 370
 - mass storage 482
 - mirrored volumes 479
 - multiple network adapters 427
 - RAID-5 volumes 479
 - Removable Storage-aware applications 65 – 66
 - storage devices and media, Remote Storage 95
 - System Monitor 236 – 241
 - Task Manager 250 – 251
 - TCP/IP ports 183 – 184
 - volumes, local storage 94
 - Windows 2000 588
 - Windows 2000 UPS service 489
 - write-back cache 149
- Connections
 - clients, testing with NUL port 177
 - continuous 190
 - disrupted network connections 490 – 491

Connections (*continued*)

- job-based 190 – 191
- NetWare printer shares 200
- print servers, adding with rundll32 217
- printer 165
- troubleshooting 578, 607
- troubleshooting cables and connectors 43

Consistency

- databases, maintaining 71
- logon scripts 519

Context Blocks Queued/sec counter 408

Context switches

- monitoring 338 – 339, 438
- running threads 348 – 349

Context Switches/sec counter 328 – 329

Contingency planning, system recovery 454 – 456

Continuous connections 190

Control registry subkey 593 – 595

Control sets, selecting 623 – 624

Controller caches, deciding to enable 149

Controls, ActiveX 282 – 288

Convert tool 155 – 156

Copy backup 495

Copy command

- Recovery Console 533
- using wildcards with 128

Copying files

- effects of compression upon 143 – 146
- NTFS, to floppy disks 118
- premigrated 86 – 87
- preserving permissions 139
- Recovery Console 530
- to volumes almost full 146
- wildcards 128

Copying placeholders 86 – 87

Costs, replacement 456

Counters

- % Disk Read Time 373
- % Disk Time 263, 373
- % Disk Write Time 373
- % Free Space 263, 371
- % Idle Time 373
- % Net Utilization 263
- % Processor Time 253, 256, 263
- % Usage 263
- analyzing memory usage 302
- Application-Layer objects 404 – 409
- Available Bytes 257, 263
- averaging 232

Counters (*continued*)

- Avg. Disk Bytes/Read 380
- Avg. Disk Bytes/Transfer 371
- Avg. Disk Bytes/Write 380
- Avg. Disk Queue Length 372
- Avg. Disk sec/Read 380
- Avg. Disk sec/Transfer 372
- Avg. Disk sec/Write 380
- Browser object 404 – 405
- Bytes Printed/sec 213
- Bytes Total/sec 264
- cache 318 – 321
- Cache Bytes 257
- choosing groups of for monitoring 242
- Commit Limit 257
- Committed Bytes 256 – 257
- Current Disk Queue Length 263, 372
- Disk Bytes/sec 372
- Disk Read Bytes/sec 380
- Disk Reads/sec 263, 380
- Disk Transfers/sec 372
- disk usage monitoring 387
- Disk Write Bytes/sec 380
- Disk Writes/sec 263, 380
- disks 370 – 380
- Free Megabytes 372
- Handle Count 256
- Handle Count measure 253
- highlighting data for 242
- ID Process 255
- instantaneous 232
- Interrupts/sec 264
- IO Other Bytes/sec 253
- IO Other Operations/sec 253
- IO Read Operations/sec 253
- IO Write Bytes/sec 254
- IO Write Operations/sec 254
- IP Read Bytes/sec 253
- Job Errors 213
- Memory 312
- Memory\Available Bytes 305, 311
- Memory\Pages/sec 305
- missing, troubleshooting 268
- monitoring performance with 433
- monitoring printer performance 213
- monitoring processor activity with 331, 333 – 334
- NBT Connection object 404
- Network Interface objects 399 – 400
- Network Protocol objects 401 – 403

Counters (*continued*)

- Network Segment objects 400 – 401
- Pages/sec 263
- paging activity monitoring 386
- performance monitoring 230 – 232, 259 – 260
- Performance, backing up configurations 515
- Pool Nonpaged Bytes 254, 257
- Pool Paged Bytes 254, 257
- Priority Base 252
- Private Bytes 255
- Process 305, 311 – 312, 328
- Processes 257
- processor 328
- Processor Queue Length 264, 334 – 337
- Processor% Processor Time 434 – 435
- Queue Length 264, 388
- read and write measurements 380, 386
- recommended thresholds 263 – 264
- Redirector object 406
- Server object 407 – 409
- Server Work Queues object 409 – 412
- Server Work Queues\Queue Length 337
- Split IO/sec 373
- system 328
- System\Interrupts/sec counter 332
- System Monitor, counterparts to Task Manager counts 256 – 257
- System\Processor Queue Length 435 – 436
- Task Manager Process measures 252 – 255
- Task Manager, System Monitor counterparts 256 – 257
- testing maximum throughput 378
- thread 328, 329
- Thread Count 255, 257
- using to establish baselines for disk usage 382
- viewing descriptions, System Monitor 241
- Work Item Shortages 264
- Working Set 254
- zero values, troubleshooting 267

CPU *See* Central processing units

CPU gauge 250

CPU Time measure 253

CPU Usage count 256

CPU Usage measure 253

CPUStres tool 330

Ctrlist.exe 258

Current Bandwidth counter 400

Current Commands counter 407

Current Disk Queue Length counter 263, 372

Current entry 591

Customizing Windows 2000 588

D

Daily backup 495

Damaged boot sectors 38 – 41

Damaged data, recovery and restoration planning 454

Damaged disk Stop messages 650, 654

Damaged drivers

- finding with /SOS switch 628

- Stop 0x24 message 650

- Stop 0x7A message 661

- Stop 0xC0000221 message 669

Damaged files

- Stop 0x24 message 650

- Stop 0x50 message 656

- Stop 0xC0000221 message 669 – 671

Damaged Master Boot Record

- running Recovery Console 528

- troubleshooting 38 – 41

- viruses 35 – 38

Data

- backing up *See* Backups

- collecting, architecture for 226 – 232

- compression *See* File compression

- missing, troubleshooting 267

- random and sequential access 391

- recovery

- mirrored volumes 476

- NTFS 148 – 149

- recovery and restoration planning 454

- Remote Storage 100 – 101, 551 – 559

- restoring from backups 546

- storage

- Disk Management snap-in 49, 101 – 102

- disk quotas *See* Disk quotas

- overview 47 – 49

- Remote Storage *See* Remote Storage

- Removable Storage *See* Removable Storage

Data attribute type 126

Data Link layer 397

Data property 240

Data streams

- description 414

- NTFS 118

Data types

- LPD utility 194 – 195

- NT EMF 1.00x, print processors 175

Data types (*continued*)

- Print Server for Macintosh 201 – 202
- PSCRIPT1, Print Server for Macintosh 201
- RAW
 - print processors 175
 - Print Server for Macintosh 201
 - printer server service 172
- TEXT, print processors 176
- DATA_BUS_ERROR Stop message 652 – 654
- Databases
 - COM+ registration database, restoring 544 – 545
 - Exchange, backing up and restoring 522 – 523
 - Jet, restoring 552
 - registration, backing up 515
 - Remote Storage, backing up 521
 - Removable Storage
 - backing up and restoring 71 – 72
 - overview 51
- Date stamp, disabling NTFS 368
- Decision tree 422
- Decommissioned state 61
- Decommissioning volumes 87
- Decreasing cluster size, FAT32 volumes 115
- Defects, hardware 658
- Deferred procedure calls (DPCs)
 - activity rates, monitoring 437
 - description 431
 - partitioning 440 – 442
- Defragmentation of disks 453, 375
- Del command
 - Recovery Console 533
 - using wildcards with 128
- Delegating backup-and-restore operations 508
- Delete command, Recovery Console 533
- Deleting
 - audit entries for printers 214
 - files
 - preventing 140
 - with wildcards 128
 - multiple disk sets 8
 - orphans, printers 206 – 207
 - placeholders 86
 - premigrated files 86
 - third-party remote control programs 649
- DependOnGroup registry entry 594
- DependOnService registry entry 594
- Designing applications for optimal performance 443 – 445
- Desired Free Space 79, 82

Detail pane 421

Device drivers

- Dmio.sys disk driver 101
- finding missing or corrupt 628
- Ftdisk.sys disk driver 101
- initializing 624
- loaded at startup
 - displaying while loading 628
 - drivers in Boot.ini 620 – 621
 - drivers in partition table 14
 - errors 625
 - kernel load phase 623
 - loading process 624
- printer *See* Printer drivers
- protected mode disk drivers 36
- Remote Storage 91
- SCSI *See* Small computer system interface
- troubleshooting
 - boot device driver errors 41
 - device initialization failures 628 – 629
 - Device Manager 574 – 575
 - Drivers utility 612
 - failed boot device driver 663
 - Hardware wizard 572
 - kernel drivers 296, 316
 - Knowledge Base 586
 - Removable Storage 77 – 78
 - resolving Stop message errors 647
 - startup problems 628 – 629
 - Stop 0x1E message 649
 - Stop 0x2E message 653
 - Stop 0x7F message 667
 - Stop 0xA message 647
 - Stop 0xC000021A message 668
 - testing in safe mode 629 – 633, 645
 - Windows 2000 compatibility 604
- uninstalling 577
- video cards 487
- viewing in Computer Management snap-in 567 – 570
- viewing order loaded and initialized 594
- Windows Update 577
- Device Manager tool 574 – 575
- Dfs (Distributed file system) 374
- DHCP (Dynamic Host Configuration Protocol) 610
- Differential backups 495, 516 – 517
- Digital signature, system files 573
- Digital video disk (DVD) 130, 59
- Dir command, Recovery Console 533

- Directing output
 - 16-bit applications 192 – 193
 - LPR (line printer remote) utility 194
 - NetWare clients 199
- Directories *See* Folders
- Directory encryption, NTFS 119
- Directory records, NTFS 125
- Directory services, restoring backup 546
- DirectX Diagnostic tool, troubleshooting with 572
- DirUse tool 157
- Disable command, Recovery Console 534
- Disabling BIOS 481
- Disabling disk counters 371
- Disaster planning, data recovery 454
- Disk bottlenecks 291
- Disk Bytes/sec counter 372
- Disk cabling, Stop 0x7A message 661
- Disk Cleanup tool 571
- Disk controllers
 - avoiding failures 487
 - deciding to enable 149
- Disk Groups
 - adding new disk to group 469 – 471
 - description 467
 - moving disks between computers 468 – 469
- Disk Management attribute, Remote Storage 82 – 83
- Disk Management snap-in
 - configuring striped volumes 472 – 473
 - creating mirrored and RAID-5 volumes 479 – 480
 - disk configuration database 10, 12
 - displaying volume status 465 – 467
 - dynamic disk management *See* Dynamic disks
 - formatting NTFS volumes, cluster sizes 123
 - legacy volume support 8
 - managing data storage 49, 101 – 102
 - moving disks between computers 468 – 469
 - outputting disk configuration information 457
 - unknown volumes 42
 - volume property sheets 94
- Disk paging file *See* Memory
- Disk quotas
 - disk space queries 120 – 121
 - implementing 102 – 107
 - limit exceeded 107
 - overview 49
 - using in Windows NT 122
 - using to tracking disk space 107
- Disk Read Bytes/sec counter 380
- Disk Reads/sec counter 263, 380
- Disk space
 - auditing 107
 - checking amount available 78
 - checking compressed file disk usage 157
 - counters for measuring 371 – 373
 - free, quotas and 103 – 104
 - mirrored volumes 476
 - monitoring 374 – 375
 - querying 121
 - quotas *See* Disk quotas
 - requirements for converting FAT to NTFS 156
 - servers, planning for 278
- Disk Transfers/sec counter 372
- Disk Write Bytes/sec counter 380
- Disk Writes/sec counter 263, 380
- DiskMap tool 34
- Diskpart command, Recovery Console 534
- Diskperf command, Recovery Console 370
- DiskProbe tool 10, 34
- Disks
 - accessing with Recovery Console 529
 - alignment 370
 - basic *See* Basic disks
 - configuring for optimal performance 367 – 370
 - controller errors 658, 663
 - corruption errors 650, 654
 - defragmenting 453, 375
 - dynamic *See* Dynamic disks
 - effects of page faults upon 309 – 310
 - effects of symmetric multiprocessing 433
 - Emergency Repair Process 540 – 543
 - failures
 - avoiding 487
 - mirrored volumes 476, 482
 - RAID-5 volumes 477
 - fault-tolerant *See* Fault-tolerant systems
 - initializing 6
 - magneto-optic (MO) 52
 - monitoring
 - application usage 390 – 392
 - counters for 259, 370 – 373, 371 – 380
 - disk usage 387
 - efficiency 376 – 380
 - establishing baselines 381 – 384
 - I/O requests queued for service 388
 - investigating problems 385 – 388
 - recommended counter thresholds 263
 - resolving bottlenecks 389
 - space 374 – 375

Disks (*continued*)

- recovering and restoring configurations 546
 - sectors critical to startup 10 – 33
 - space *See* Disk space
 - spreading paging files across 299
 - startup 616, 617
 - storage 331
 - troubleshooting 34 – 43, 385 – 388
 - unsupported, Stop message 663
 - verifying integrity 658, 661, 664
- Disrupted network connections, causes of 490 – 491
- Distributed file system (Dfs) 374
- Distributed link tracking 121
- Distributed Transaction Coordinator object 228
- DLL files, corrupt 669
- Dmio.sys disk driver 101
- Document management programs, Remote Storage-aware 99
- Documenting backup-and-restore procedures 511
- Documenting recovery procedures 461
- DOS *See* MS-DOS
- DoubleSpace tool 141, 147
- DPC *See* Deferred procedure calls
- Dr. Watson for Windows 2000 tool 571
- Drive is too small message, mirrored volumes 481
- Driver Verifier for testing kernel drivers 296
- Drivers
- device *See* Device drivers
 - Network Monitor *See* Network Monitor
 - printer *See* Printer drivers
- Drivers utility 612
- Drives
- cleaning, Removable Storage 75
 - in libraries 53
 - mappings 530
 - spreading paging files across 299
 - stand-alone 54
 - states of 77
- DriveSpace tool 141, 147
- Duplexed mirrored volumes 474, 475
- Duplicate media, handling with Removable Storage 59
- DVD-ROM 130, 59
- Dynamic disks
- converting basic disks 468
- Disk Groups
- adding new disk to group 469 – 471
 - description 467
 - moving disks between computers 468 – 469
- features 8 – 10

Dynamic disks (*continued*)

- managing data storage with 102
 - overview 5 – 7
 - simple volumes 471
 - spanned volumes 471 – 472
 - starting Windows 2000 from 22
 - upgrading basic disks to 5, 7
- Dynamic Host Configuration Protocol (DHCP) 610
- Dynamic priorities, monitoring 357

E

- EBR (extended boot record) 19 – 21
- Efficiency of disks, monitoring 376 – 380
- EFS (Encrypting File System) 119
- EIDE (Enhanced Integrated Drive Electronics) devices 43, 481
- EISA volumes 482
- Ejecting media in Removable Storage 73 – 74
- Emergency Repair Process
- Emergency Repair Disk, creating 541 – 542
 - Emergency Repair Disk, using 634
 - moving disks between computers 635
 - overview 540 – 541
 - registry files 541
 - repairing damaged boot sectors 39
 - repairing Windows 2000 installations 542 – 544
 - Setup floppy disks 462
- Empty disks, initializing 6
- Enable command, Recovery Console 535
- Encrypted files
- not valid in Windows NT 122
 - restoring 518
- Encrypting File System (EFS) 119
- End of sector markers 21
- Ending Cylinder field 15 – 18
- Enhanced Integrated Drive Electronics (EIDE) devices 43, 481
- Enum registry subkey 593
- Enumerating volumes 158
- Error and Event Messages Help 584 – 585
- Error detection, RAM 486 – 487
- Error events 583
- Error messages
- Access is denied 530
 - Error and Event Messages Help 584 – 585
 - Stop messages *See* Stop messages
 - troubleshooting 604
- ErrorControl registry entry 594

- Error-corrective coding (ECC) 486
- Errors System counter 408
- Estimating replacement costs 456
- Event ID 410 – 412, 427
- Event Viewer 582 – 584
- Events
 - Application log 582
 - auditing print events 214
 - Error and Event Messages Help 584 – 585
 - logging disk quota limits 107
 - logging spooler events 216 – 217
 - Security log 583
 - starting Event Viewer 582
 - System log 582
 - tracing 231
 - Troubleshooters 585 – 586
 - types of 583
 - viewing in Event Viewer 583 – 584
- Exceeding disk quota limits 107
- Excel, placing System Monitor ActiveX control in spreadsheets 283 – 286
- Exchange, backing up and restoring 522 – 523
- Exctrlst.exe 258
- Execute Command Line trigger 420
- Exit command, Recovery Console 535
- Expand command, Recovery Console 535
- Expand tool 157
- Explorer integration with Remote Storage 93
- Exporting logs to spreadsheets 249
- Extended BIOS parameter block
 - boot sector 22, 24
 - FAT16 volumes 24
 - FAT32 volumes 27, 29
 - NTFS volumes 31 – 33
- Extended boot record (EBR) 19 – 21
- Extended Boot Signature field 27 – 31
- Extended Flags field 29
- Extended Industry Standard Architecture (EISA) volume 482
- Extended partitions
 - basic disks 8
 - dynamic disks 9, 9 – 10
 - extended partition table 19 – 21
 - partition table information 12
 - upgraded from basic storage 7
- Extended volumes
 - limitations of 10
- External application libraries 91

F

- Failed entry 591
- Failed state 57
- Failovers, Print Spooler resources 213
- Failure Audit events 583
- Failures
 - boot devices, Stop 0x7B message 663
 - categorizing 455
 - disk
 - mirrored volumes 474, 482
 - RAID-5 volumes 477
 - recovery from, mirrored volumes 476
 - hardware
 - avoiding 486 – 487
 - Stop 0x50 message 655
 - Stop 0x7F message 666 – 667
 - mean time between 455
 - memory
 - Stop 0x77 message 658
 - Stop 0xC0000221 message 671
 - motherboard 486
 - MTBF 487
 - probabilities of 455
 - RAM 661
 - recovery plans
 - developing 459 – 461
 - training personnel 462
 - single points of, avoiding 485 – 491
 - Windows 2000 startup 615
- Fast Repair option, Emergency Repair Process 542 – 543
- Fastfat driver 115
- FAT12 file system 112
- FAT16 file system
 - boot sectors 24 – 25
 - cluster sizes 17, 112
 - compared to FAT32 130 – 133
 - compared to NTFS *See* NTFS file system
 - converting to NTFS 121, 155 – 156
 - file names 116 – 117
 - floppy disks 112
 - maximum cluster size 17
 - maximum volume size 112, 136
 - moving and copying files to NTFS volumes 145
 - operating system compatibility 111
 - overview 111 – 114
 - scalability 115
 - using in Windows 2000 117
 - volume structure 113 – 114

- FAT32 file system
 - BIOS parameter block (BPB) structure disabled 115
 - boot sectors 27 – 29
 - cluster sizes 17, 115
 - compared to FAT16 130 – 133
 - compared to NTFS *See* NTFS file system
 - converting to NTFS 121, 155 – 156
 - extended attributes disabled 115
 - file names 116 – 117
 - logical drive size 115
 - maximum cluster size 17
 - maximum file size 115
 - maximum volume size 114, 115, 136 – 137
 - moving and copying files to NTFS volumes 145
 - operating system compatibility 111
 - overview 114 – 116
 - scalability 115
 - using in Windows 2000 117
 - volume structure 115 – 116
- Faults, page 291, 306 – 310
- Fault-tolerant systems
 - backups 523
 - climate control system 451
- Disk Groups
 - adding new disk to group 469 – 471
 - description 467
 - moving disks between computers 468 – 469
- dynamic storage 6, 8
- Ftdisk tool 102
- hardware vs. software 484 – 485
- mass storage systems 482 – 484
- mirrored volumes *See* Mirrored volumes
- page file location 482
- planning considerations 451 – 452, 485 – 486
- RAID configurations 465 – 467
- RAID-5 volumes *See* RAID-5 volumes
- testing 485
- Fdisk command
 - setting partitions 39
 - troubleshooting viruses with 38
- Fields
 - FAT16 volume partition tables 25
 - FAT32 volume partition tables 29
 - NTFS volume partition tables 32
- File allocation table (FAT)
 - FAT16 *See* FAT16 file system
 - FAT32 *See* FAT32 file system
 - Stop 0x77 message 658
- File allocation table (FAT) (*continued*)
 - Stop 0x7A message 661
 - Stop 0x7B message 664
- File and Print Services 173, 198 – 199
- File attributes, NTFS 126
- File compression
 - Compact tool 143, 153 – 154
 - Compress tool 154 – 155
 - compressed object color 143
 - compressing files 142
 - compression algorithm 141, 146
 - compression utilities 147
 - copying compressed files 143, 145 – 146
 - decompressing files 142
 - determining disk space usage 157
 - determining file size 157
 - disk quotas 104
 - DoubleSpace tool 141, 147
 - DriveSpace tool 141, 147
 - effect on disk space 104
 - effect on performance 147
 - Expand tool 157
 - moving compressed files 143 – 146
 - NTFS support 133, 141
 - page files 142
 - reading compressed files 141
 - setting folder compression state 141 – 142
 - volumes low on free disk space 154
- File encryption, NTFS 119
- File name attribute type 126
- File names
 - CD-ROM 130
 - disabling short 368
 - FAT volumes 116 – 117
 - generating short 128 – 129
 - log files (Performance Logs and Alerts) 249
 - long names
 - Stop 0x77 message 658
 - Stop 0x7A message 661
 - Stop 0x7B message 664
 - using 127 – 129
 - NTFS volumes 127
 - POSIX 140 – 141
 - spaces in 127 – 128
 - viewing 129
- FILE port 177
- File records, NTFS 125
- File Selection Criteria 79
- File Signature Verification Utility 573

File System Information Sector Number field 29

File System Type field 27 – 31

File System Version field 29

File systems

compact disc file system (CDFS) 130

compared 130 – 141

FAT16 *See* FAT16 file system

FAT32 *See* FAT32 file system

NTFS *See* NTFS file system

operating system compatibility 111

supported in Windows 2000 109 – 111

tools for working with

Cacls 152 – 153

Compact 153 – 154

Compress 154 – 155

Convert 155 – 156

DirUse 157

Expand 157

Mountvol 158

Universal Disk Format (UDF) 130

FILE_FLAG_BACKUP_SEMANTICS flag 80

FILE_FLAG_OPEN_BACKUP_SEMANTICS parameter 98

FILE_FLAG_OPEN_NO_RECALL flag 80, 85 – 86

FILE_OPEN_NO_RECALL parameter 99

Files

backing up *See* Backups

Boot.ini *See* Boot.ini

command files, running during power failures 489

compressing *See* File compression

controlling access to *See* Access control lists

copy command

Recovery Console 530

wildcards 128

databases *See* Databases

deleting with wildcards 128

encrypted, restoring 518

grouping 88

location in FAT16 volumes 114

locked 518

managing using Remote Storage *See* Remote Storage

managing using Removable Storage *See* Removable Storage

names *See* File names

NTFS *See* NTFS file system

optimizing performance 367 – 370

POSIX 140 – 141

preventing deletion of 140

Files (*continued*)

printcap, viewing 196

replicating 88

required to start Windows 2000 615, 617

restoring from backups 546

signature files, antivirus programs 37

sizes 115

sparse

NTFS support 119 – 120

using in Windows NT 122, 123

speed of reading and writing in Windows 2000 135

stored in MFT 124

system mismatches, Stop 0xC000021A message 669

Filter Item options 422

Filtering events 583

Filtering frames 422

Fixboot command, Recovery Console 536

Fixmbr command, Recovery Console 38, 536

Flow meter capacity metric, Remote Storage 88 – 89

Flushing caches 320

Folders

accessing in Recovery Console 530

Active Directory, backing up 514

cataloging and viewing those available 558

compressing *See* File compression

controlling access to 138 – 140

in registry editor 588

MFT records 125

Repair 541

structure

FAT16 volumes 113 – 114

FAT32 and NTFS volumes 115 – 116

volume mount points 150

Fonts property, System Monitor 240

Forcing printer restart 207

Foreground process scheduling 356

Format command, Recovery Console 536

Formatting

FAT16 volumes 112

FAT32 volumes 115

NTFS volumes 124 – 125

System Monitor ActiveX controls in documents 286 – 288

Forwarding local print jobs 181

Fragmentation of disks 375, 391

Frame Viewer window 421

Free media 63 – 65

Free Megabytes counter 372

Free pools 55, 64
FrontPage, inserting System Monitor ActiveX control in 286
Ftdisk tool 102, 474
Ftdisk.sys disk driver 101
Full partitioning 438
Full Remote Storage 90

G

Gateway Service for NetWare 173, 199 – 200
Gauges, CPU 250
GDI (Graphical Device Interface) 169
GDI objects measure 253
General property 240
Globally unique identifiers (GUID)
 description 558
 naming media with, Removable Storage 58
Graph pane 417
Graph property 241
Graphical Device Interface (GDI) 169
Graphing processor time in privileged and kernel modes 256
Graphs, System Monitor 242
Group policy printer settings 208 – 209
Grouping files 88
Groups, choosing for monitoring 242
GUID *See* Globally unique identifiers

H

HAL *See* Hardware abstraction layer
Hal.dll, Stop 0x79 message 659
Handle Count counter 253, 256
Hard disks
 accessing with Recovery Console 40
 bad blocks, Stop 0x24 message 650
 integrity
 Stop 0x77 message 658
 Stop 0x7A message 661
 Stop 0x7B message 664
 startup disks as 616
Hard page faults 291, 306 – 310
Hard processor affinity 439
Hard quota limit, disk quotas 104
Hardware
 compatibility 604
 components, avoiding failures 486 – 487
 defective 658

Hardware (*continued*)
 detecting at startup 622
 failures
 Stop 0x50 message 655
 Stop 0x7F message 666 – 667
 incompatibility
 Stop 0x1E message 649
 Stop 0x7B message 663
 Stop 0x7F message 666 – 667
 installing, Stop message 649
 media-moving 50
 Stop 0x2E message 652 – 653
 troubleshooting startup problems with 628 – 629
 upgrade planning 453 – 454
Hardware abstraction layer (HAL)
 error messages 672
 mismatched 659 – 660
Hardware Compatibility List (HCL) 606 – 607
Hardware interrupt partitioning 442
Hardware malfunction messages 639, 672 – 673
Hardware Profiles subkey 593
Hardware RAID, Windows 2000 compatibility 467
HARDWARE registry key 589
Hardware Resources, System Information tool 568
Hardware troubleshooter 575
Hardware Wizard 572
HCL (Hardware Compatibility List) 606 – 607
Head field 15 – 18
Headers, protocol 397
Heartbeat thread 279
Hex pane 421
Hidden Sectors field 25 – 29
Hiding Task Manager button 251
High class 354
Highlighting data 242
Histograms, System Monitor 236
HKEY_CLASSES_ROOT subtree 587
HKEY_CURRENT_CONFIG subtree 587
HKEY_CURRENT_USER subtree 587
HKEY_LOCAL_MACHINE subtree
 description 587
 keys in 589 – 591
HKEY_USERS subtree 587
Holes 146
Host names, entering printer addresses 196
Hot fixes, uninstalling 577
HP Network Print Monitor (Hpmon) 190 – 191
HP-GL/2 Plotter Driver 171
Hpmon *See* HP Network Print Monitor

-
- HTML *See* Hypertext Markup Language
 - HTTP Indexing Service object 228
 - Hubs as cause of disrupted network connections 490 – 491
 - Hypertext Markup Language (HTML)
 - displaying printing information 187
 - installing printers 186 – 187
- I**
- I/O *See* Input/output
 - I/O Other Bytes measure 253
 - I/O Other measure 253
 - I/O Read Bytes measure 253
 - I/O Reads measure 253
 - I/O status code
 - Stop 0x77 message 657, 658
 - Stop 0x7A message 661
 - I/O Write Bytes measure 254
 - I/O Writes measure 254
 - IAS Accounting Clients object 228
 - IAS Accounting Servers object 228
 - IAS Authentication Clients object 228
 - IAS Authentication Servers object 228
 - ICMP object 228
 - Icons, CPU gauge 250
 - ID Process counter 255
 - IDE drivers, corruption 650
 - Ideal processor 438
 - Identifiers, GUID 558
 - Idle priority class 354
 - Idle process 330
 - Idle state 61
 - IE ports *See* Insert/eject ports
 - IIS *See* Internet Information Service
 - Image Name measure 254
 - ImagePath registry entry 594
 - Import pools 56, 64
 - Imported state 61
 - In Process state 57
 - In Use state 61
 - Inaccessible boot device error 41
 - Inaccessible state 61
 - INACCESSIBLE_BOOT_DEVICE Stop message 662 – 664
 - Incompatible hardware
 - Stop 0x1E message 649
 - Stop 0x7B message 663
 - Stop 0x7F message 666 – 667
 - Incompatible state 61
 - Incremental backups 495, 516 – 517
 - Index Allocation attribute type 126
 - Index Root attribute type 126
 - Indexing Service Filter object 228
 - Indexing Service object 228
 - Information events 583
 - Inheritable permissions 138
 - Initial sizes of paging files, setting 298
 - Initializing
 - device drivers 624
 - kernels 624 – 625
 - new and empty disks 6
 - InoculateIT AntiVirus AVBoot program 575
 - Input/output (I/O), sizes of requests 391 – 392
 - Insert/eject (IE) ports in libraries 54
 - Inserting media, Removable Storage 73 – 74
 - Inspect Boot Sector option 543
 - Inspect Startup Environment option 543
 - Installed memory, determining amount of 292 – 293
 - Installing
 - applications 604
 - client drivers, Windows 95 and 98 191
 - device drivers, Stop 0x2E message 653
 - hardware, Stop 0x1E message 649
 - Hpmon 190 – 191
 - Network Monitor 415 – 416
 - Print Server for Macintosh 193, 201
 - print shares 178 – 179, 181
 - printers *See* Printers, installing
 - PrnAdmin tool 219
 - Remote Storage 95
 - Removable Storage-aware applications 65 – 66
 - standard TCP/IP port with SPM 183 – 184
 - Windows 2000
 - limitations of dynamic disks when 9
 - Stop messages 642, 647
 - Instances
 - _Total 231
 - choosing groups of for monitoring 242
 - loopback addresses 399
 - missing, troubleshooting 268
 - performance monitoring 230 – 232
 - tracking totals of, System Monitor 242
 - Instantaneous counters 232
 - Integrated Windows authentication option 189
 - Integrating ActiveX control into applications 282 – 288

Integrity
 hard disks, verifying 658, 661, 664
 NTFS volumes 148
Intermediary devices 490 – 491
Internet
 printing 166, 185 – 189
 Web pages, placing System Monitor ActiveX control into 283 – 286
Internet Explorer
 System Information tool 571
 viewing and managing printers 166
Internet Information Service (IIS) 166, 173
Interprocessor interrupt 437
Interrupt avoidance 338
Interrupt moderation 338, 441 – 442
Interrupt Request Level (IRQL)
 deferred procedure calls 431
 Stop message 646
Interrupts
 activity rates 437
 effects upon bottlenecks 332
 monitoring 337 – 338
 software *See* Deferred procedure calls
Interrupts/sec counter 264, 328
Inventories, Removable Storage 75
IO Other Bytes/sec counter 253
IO Other Operations/sec counter 253
IO Read Operations/sec counter 253
IO Write Bytes/sec counter 254
IO Write Operations/sec counter 254
IP object 228
IP Read Bytes/sec counter 253
IPConfig tool 578 – 579, 609 – 610
IPI *See* Interprocessor interrupt
IPSecMon tool 581
IrDA (Infrared) ports 180
IRQL (Interrupt Request Level)
 deferred procedure calls 431
 Stop message 646
IRQL_NOT_LESS_OR_EQUAL Stop message 646 – 648
Isolating sources of problems 602

J

Jet databases, restoring 552
Job Errors counter 213
Job Object 228, 329

Job Object Details object 229
Job-based connections 190 – 191

K

Kernel mode *See* Privileged mode
Kernel Stop messages 584
KERNEL_DATA_INPAGE_ERROR Stop message 660 – 662
KERNEL_STACK_INPAGE_ERROR Stop message 657 – 659
Kernel-level drivers, Remote Storage support 91
Kernel-mode memory leaks 316
Kernels
 context switches, monitoring 338 – 339
 displaying 628
 initializing 624 – 625
 loading 623 – 625
 mismatches 659 – 660
KMODE_EXCEPTION_NOT_HANDLED Stop message 648 – 650
Knowledge Base 586, 608

L

LAN backups 501
Language monitors 176
Laptop computers
 dynamic disk support 9
 troubleshooting problems with 613
Large backups 503
Large Sectors field 25 – 29
Large sites, granting rights at 499
LargeSystemCache registry entry
 changing 294
 optimizing memory 296
 values 295
Last Known Good Configuration 633, 647
LastKnownGood configuration 591 – 592
Lazy-write technique 149
Leaks (memory)
 identifying 310 – 315
 kernel-mode 316
 nonpaged pools 312 – 313
LeakyApp tool
 counter activity during memory leaks 314
 paging file usage during memory shortages 300
Legacy applications, monitoring 278 – 282
Legacy network interfaces, printing 190 – 191

- Legacy volumes 8
 - Legends, System Monitor 235, 241
 - Libraries
 - overview 53 – 54
 - Remote Storage, upgrading 90
 - robotic, configuring 69
 - sharing with external applications 91
 - single and multiple tape, Remote Storage 78
 - states of 77
 - technical reference, creating 457
 - troubleshooting 78
 - License management, Remote Storage 95
 - Limiting log size 249
 - Line printer daemon (LPD) utility 193 – 198
 - Line printer remote (LPR) utility 193 – 198
 - Links, slow 402 – 403
 - Links, tracking in NTFS 121
 - Listsvc command, Recovery Console 536
 - Load balancing and scaling 445 – 446
 - Local area networks (LANs), backups 501
 - Local computers
 - backups 496 – 497, 518
 - enabling disk quotas on 106
 - Local only mode 415
 - Local port monitors (Localspl.dll) 177 – 178
 - Local print providers, Windows 2000 servers 173 – 175
 - Local printing
 - forwarding print jobs 181
 - installing print shares 178 – 179
 - overview 162 – 165
 - Local Stop files, creating 598
 - Local storage
 - configuring and managing volumes 94
 - managing with Remote Storage 82
 - monitoring management of 95
 - NTFS files 85 – 88
 - Localspl.dll *See* Local port monitor
 - Locked files, backing up 518
 - Log File Service, redo and undo information 149
 - Log files, backup-and-restore procedures 511
 - Log services, scheduling monitoring with 331
 - Logged Tool Stream attribute type 126
 - Logging
 - Application log 582
 - processor usage per thread 347 – 348
 - Security log 583
 - spooler events 216 – 217
 - System log 582
 - time used by processes 340 – 344
 - Logging (*continued*)
 - transactions, NTFS 148 – 149
 - viewing event logs in Event Viewer 582, 583 – 584
 - Logging on to finish Windows 2000 startup 615
 - Logical Disk counter 331
 - Logical Disk Manager 102
 - Logical identifiers 52
 - Logical printer 161
 - Logical volumes 523
 - LogicalDisk object
 - counters 371 – 373
 - description 229, 370 – 371
 - Logon command, Recovery Console 536
 - Logon process 625
 - Logon scripts, backing up 518 – 519
 - Logs
 - event *See* Events
 - Performance Logs and Alerts *See* Performance Logs and Alerts
 - Long file names
 - FAT volumes 116 – 117
 - generating short names from 128 – 129
 - overview 127 – 129
 - spaces in 127 – 128
 - Stop 0x77 message 658
 - Stop 0x7A message 661
 - Stop 0x7B message 664
 - viewing 129
 - Loopback addresses 399
 - Loss of data, recovery and restoration planning 454
 - LPD (line printer daemon) utility 193 – 198
 - LPR (line printer remote) utility 193 – 198
 - LPR protocol, remote printing 182 – 183
 - LPT, detecting print device on 180
- ## M
- Machine types, mismatches 659 – 660
 - Macintosh computers
 - Printer Server for 173
 - printing from clients 200 – 203
 - SFM volumes, Stop 0x24 message 651
 - Magneto-optic (MO) disks 52
 - Mailslot Allocations Failed counter 404
 - Mailslot Opens Failed/sec counter 404
 - Mailslot Receives Failed counter 404
 - Mailslot Writes Failed counter 405
 - Managed files, recovering 557 – 558

Managing data storage

- Disk Management tool 49, 101 – 102
- disk quotas *See* Disk quotas
- overview 47 – 49
- Remote Storage *See* Remote Storage
- Removable Storage *See* Removable Storage

Managing volumes 94

- Manual configuration, Removable Storage 69 – 70
- Manual publishing, printers 206
- Manual Repair option, repairing system files 542 – 543
- Map command, Recovery Console 537
- Map requests, NTFS files 85
- Mapping, volumes 530
- Mass storage, configuring 482
- Master boot code 11
- Master boot record (MBR)
 - extended boot record (EBR) 19 – 21
 - location 10
 - overview 11 – 21
 - repairing damaged 38 – 41
 - role in initial Windows 2000 startup 616
 - running Recovery Console when damaged 528
 - viruses 35 – 38

Master File Table (MFT)

- moving 31
- NTFS volumes 124 – 125

Master media, recreating 558

MasterPeriodicity parameter 406

MaxGlobalOpenSearch counter 412

MaxHashTableSize registry subkey 420

Maximize Data Throughput for File Sharing option 306

Maximum throughput testing 378 – 379

MaxKeepSearch counter 412

MaxUserPort registry subkey 420

MBR *See* Master boot record

Md command, Recovery Console 537

Meantime between failures (MTBF) 455, 487

Measuring processor performance *See* Processors, monitoringMeasuring SMP performance *See* Symmetric multiprocessing

Media

- backup 500 – 501, 517
- free 63 – 65
- handling 60
- identifying and naming 58 – 60
- labels, backup-and-restore procedures 511
- offline, physical locations of 54

Media (*continued*)

- preparing 66
- protecting tape cartridges 100
- recovering 558 – 559
- Remote Storage
 - configuring and managing 95
 - protecting 521 – 522
 - purpose of 520
 - status and location 90

Removable Storage

- backup media 71 – 72
- inserting and ejecting 73 – 74
- overview 52 – 53
- troubleshooting 78
- types 495 – 496

Media Descriptor field 25 – 29

Media pools 55 – 56, 64 – 65

Media states 61

Media-moving hardware 50

Media-sense network adapters 395

MEM Usage count 256

Memory

- bottlenecks, resolving 322 – 323
- checking amount available 78
- checking installed 293
- determining amount of installed 292 – 293
- effects of SMP on 433
- effects of virtual memory on 301
- error detection 486 – 487
- error-corrective coding (ECC) 486
- failures

- Stop 0x77 message 658
- Stop 0x7A message 661
- Stop 0xC0000221 message 671

file system cache

- bottlenecks 322 – 323
- cache counters, analyzing values 320 – 321
- cache counters, described 318 – 320
- description 293, 316
- memory and cache usage 289 – 323
- monitoring, overview 316 – 318
- optimizing 322
- setting size 293 – 295

leaks

- description 310
- kernel-mode 316
- nonpaged pools 312 – 315
- user-mode memory leaks 310 – 315

Memory (continued)

- monitoring
 - baseline, establishing 300 – 302
 - counters for analyzing memory usage 302 – 304
 - counters for monitoring performance 259 – 260
 - counters for monitoring processor activity 331
 - overview 289 – 292
 - paging activity 385 – 387
 - recommended counter thresholds 263
 - shortages 304 – 306
 - virtual memory usage 301
 - nonpaged pool, Stop 0x24 message 651
 - nonparity 486
 - optimizing 296 – 297
 - paging file
 - bad blocks messages 658, 661
 - compressing 142
 - default size 300
 - description 293
 - hard page faults 307 – 310
 - monitoring paging activity 385 – 387
 - moving 299
 - multiple 299
 - recommended counter thresholds 263
 - setting size 297 – 300
 - parity 486
 - RAID-5 volumes 479
 - reserved 293
 - services usage 301 – 302
 - setting Windows RAM usage 628
 - Windows 2000 requirements 292
- Memory dump files 482
- Memory map requests, NTFS files 85
- Memory objects
 - counters, function of 312
 - description 229
- Memory Usage Delta measure 254
- Memory Usage measure 254
- Memory.dmp, writing Stop information to 598
- Memory\Available Bytes counter 305, 311
- Memory\Pages/sec counter 305 – 306
- Memsnap 313
- Messages
 - Access is denied 530
 - drive is too small 481
 - hardware malfunction 639, 672 – 673
 - Stop *See* Stop messages
 - system 639

Metadata

- NTFS volumes 124 – 125
 - overhead, converting FAT volumes to NTFS 156
 - protecting, Remote Storage 101
- MFT *See* Master file tables
- Microsoft TechNet 566
- Migrating files
 - between NTFS folders, preserving permissions 139
 - effects of compression upon 143 – 146
- Minimizing video card failures 487
- MinKeepSearch counter 412
- Mirrored volumes
 - compared to RAID-5 475
 - configuring system partition 480 – 482
 - costs 475
 - creating 15, 479
 - deleting 549
 - disk reads and writes 380
 - disk space utilization 476
 - duplexing 474, 475
 - mass storage configurations 482 – 484
 - moving between Disk Groups 469 – 471
 - overview 474 – 476
 - recovering 547 – 549
 - replacing failed 548 – 549
 - resynchronizing 549
 - viewing status in Disk Management 465 – 467
- Mirroring partitions 475
- MISMATCHED_HAL Stop message 659 – 660
- Missed Mailslot Datagrams counter 405
- Missed Server Announcements counter 405
- Missed Server List Requests counter 405
- Missing drivers, finding with /SOS switch 628
- Mixing processor files, Stop 0x79 message 659 – 660
- Mkdir command, Recovery Console 537
- MO (magneto-optic) disks 52
- Monitoring
 - disks *See* Disks, monitoring
 - file system cache usage *See* Memory
 - I/O requests queued for service 388
 - jobs, Remote Storage 95
 - local storage, management of 95
 - memory *See* Memory, monitoring
 - paging activity 385 – 387
 - performance *See* Performance, monitoring
 - processors *See* Processors, monitoring
 - remote computers 272 – 275
 - Remote Storage 95
 - servers 275 – 278

Monitors

- Hpmon, installing 190 – 191
- language 176
- port
 - overview 177 – 178
- Sfmmon, printing documents from 203
- print
 - overview 176 – 178

More command, Recovery Console 537

Motherboards, avoiding failures 486

Mounted state 61

Mounting volume mount points 150

Mountvol tool 158

Moving files

- between NTFS folders, preserving permissions 139
- between Remote Storage installations 97
- effects of compression upon 143 – 146
- paging 299
- premigrated 86 – 87

Moving MFT 31

Moving placeholders 86 – 87, 88

MPS (Multiprocessor Specification) 441

MS-DOS

- accessing volumes, System IDs and 15
- closing searches 412
- DoubleSpace and DriveSpace compression 141
- entering long file names in 128
- Expand tool 157
- file names on FAT volumes 116 – 117
- forbidden file naming characters in 128
- monitoring MS-DOS applications 282
- printing from clients 191 – 193
- readable file names on NTFS volumes 127

MTBF *See* Meantime between failure

Multiple data streams in NTFS 118

Multiple disk sets, creating 8

Multiple network adapters, configuring 427

Multiple processors

- improving performance 332
- recommended counter thresholds for 264

Multiple tape libraries 78

Multiple-boot configurations

- FAT16 volumes 17
- formatting system partitions 134

Multiprocessor Specification (MPS) 441

Multiprocessors

- mixing files, Stop 0x79 message 659 – 660
- queue lengths 336

Multiprocessors (*continued*)**SMP system performance**

- application design and 443 – 444
- monitoring activity 433 – 438
- Network Load Balancing and scaling 445 – 446
- optimizing and tuning installations 438 – 443
- overview 431 – 433

Multithreaded applications, adding processors 342

My Computer

- changing attributes in 621
- vs. Compact tool 154

N

Name resolution, NetBIOS 580

Named streams, changing 107

Names

- file *See* File names
- host, entering printer addresses 196
- media 58 – 60
- NTVDM processes 282
- print queue 196

Natural disaster planning, data recovery 454

NBT Connection object 229, 404

NBTStat tool 580

NetBEUI protocol

- multiple network adapters 427 – 428
- NetBEUI resource objects 402

NetBIOS name resolution 580

NetDiag tool 578, 610

NetWare

- Client Service for 173
- File and Print Services for 173
- Gateway Service for 173
- NetDiag tool 578
- printing from clients and servers 198 – 200

Network adapters

- adding 427 – 428, 441, 420
- media-sense 395
- monitoring performance 399 – 400
- promiscuous mode 415
- speed 396
- switching between 420
- upgrading 441

Network cards, avoiding failures 487

Network components, effects of SMP upon 433

Network Connections tool 572

Network Errors/sec counter 407

Network Interface object 229, 399 – 400

- Network layer 397
- Network Load Balancing 445 – 446
- Network Monitor
 - captured data
 - analyzing 416
 - capture buffer 415, 425
 - capture offset 419
 - displaying 421 – 423
 - filters 418 – 419
 - frame data 416 – 421
 - reviewing 423 – 424
 - driver 396
 - installing 415 – 416
 - overview 413 – 415
- Network Monitor Capture window 417
- Network Protocol objects counter 401 – 403
- Network Segment objects counter 400 – 401
- Networks
 - bottlenecks, troubleshooting 425 – 428
 - counters for monitoring performance 260
 - disrupted network connections 490 – 491
 - improving performance over slow links 402 – 403
 - LAN, backups 501
 - monitoring performance 393 – 428
 - printers
 - Active Directory and 204 – 209
 - architecture 166 – 178
 - Cluster service 210 – 213
 - monitoring performance 213 – 219
 - non-Windows 2000 operating systems 191 – 203
 - overview 161 – 166
 - sharing 178 – 191
 - recommended counter thresholds for 263
 - sessions, viewing 418
 - traffic, monitoring processor activity affected by 331
 - troubleshooting 609 – 610
- New disks, initializing 6
- Newsgroups, receiving technical support through 566
- No Action trigger 420
- Nonpaged Pool measure 254
- Nonpaged pools
 - description 293
 - memory leaks 312 – 313
 - Stop 0x24 message 651
 - Stop 0x77 message 658
 - Stop 0x7A message 661
- Nonparity random access memory (RAM) 486
- Normal backups 495, 516 – 517
- Normal priority class 354
- Nothing trigger 420
- NT EMF 1.00x data type, print processors 175
- NT Virtual DOS Machine (NTVDM)
 - monitoring 16-bit applications 278 – 280
 - monitoring MS-DOS applications 282
 - running 16-bit applications in separate processes 281
- Ntdetect.chk 622, 627 – 628
- NTFS file system
 - adding files to volumes almost full 146
 - boot sector 31 – 32, 124
 - caching 149
 - change journal
 - description 119
 - sparse stream 119
 - using in Windows NT 122, 123
 - cluster remapping 149
 - cluster sizes 123
 - compared to FAT
 - access control features 138 – 140
 - choosing a file system 130
 - compression support 133
 - file access speed 135
 - multiple-boot systems 134
 - NFTS advantages 133 – 134
 - NFTS disadvantages 134
 - recoverability 133
 - volume sizes 136 – 137
 - compressing files and folders *See* File compression
 - converting FAT volumes 121
 - converting volumes to FAT 155 – 156
 - copying files and folders 143, 145 – 146
 - corruption
 - Stop 0x24 message 650
 - Stop 0x2E message 654
 - Stop 0x50 message 656
 - disk quotas *See* disk quotas
 - encryption
 - Encrypting File System (EFS) 119
 - using in Windows NT 122, 123
 - enumerating volumes 158
 - file attributes 126 – 127
 - file system tools, list of 151
 - files copied to floppy disks 118
 - formatting volumes 124 – 125
 - improving performance 368 – 369
 - link-tracking service 121
 - local file storage 85 – 88

NTFS file system (*continued*)

- Master File Table (MFT) 124 – 125
 - maximum volume size 137
 - metadata 124 – 125
 - monitoring disk space 374
 - moving files and folders 143 – 145
 - MS-DOS file names 127
 - multiple data streams 118
 - multiple-boot systems 122, 134
 - object identifiers
 - tracking links between files 121
 - using in Windows NT 122, 123
 - operating system compatibility 111
 - overview 117 – 127
 - POSIX compliance 140 – 141
 - recovering data 148 – 149
 - reparse points *See* Reparse points
 - sparse files
 - description 119 – 120
 - using in Windows NT 122, 123
 - upgrading to on-disk format 121
 - volume integrity 148
 - volume structure 123
 - Windows NT compatibility 122 – 123
- NTFS_FILE_SYSTEM Stop message 650 – 652
- NTLDR
- choosing operating systems from 619
 - displaying kernels and device drivers 628
 - loading kernels 623 – 625
 - role in Windows 2000 startup 617 – 618
 - troubleshooting startup problems 627
- Ntoskrnl.exe
- initializing kernels 624 – 625
 - Stop 0x79 message 659
- NTVDM *See* NT Virtual DOS Machine
- NUL port, testing client connectivity with 177
- Null sessions, forwarding print jobs 181
- Number of FATs field 25 – 29
- Number of Heads field 25 – 29
- NUMPROC=x switch 620
- NWLink protocol 401
- Nwprovau print providers 200

O

- Object ID attribute type 126
- Object identifiers, NTFS 121, 122, 123

Objects

- Browser 227, 404 – 405
- Cache 227
- Distributed Transaction Coordinator 228
- HTTP Indexing Service 228
- IAS Accounting Clients 228
- IAS Accounting Servers 228
- IAS Authentication Clients 228
- IAS Authentication Servers 228
- ICMP 228
- Indexing Service 228
- Indexing Service Filter 228
- IP 228
- Job Object 228, 329
- Job Object Details 229
- LogicalDisk
 - counters 371 – 373
 - description 229, 370 – 371
- Memory 229, 312
- missing, troubleshooting 268
- monitoring server workload 275 – 276
- NBT Connection 229, 404
- NetBEUI resource objects 402
- Network Interface 229, 399 – 400
- Network Segment 400 – 401
- Objects 229
- Paging File 229
- performance monitoring 227 – 230
- PhysicalDisk
 - counters 371 – 373
 - description 229, 370 – 371
- Print Queue 229
- Process
 - counters, function of 312
 - description 229
 - Task Manager Process measures 252 – 255
- Processor 229
- Redirector 229
- Server 230
- Server Work Queues 230
- System 230
- TCP 230
- Telephony 230
- Thread 230
- UDP 230
- Objects object 229
- Offline media, physical locations of 54
- Off-site storage, backup media 500 – 501
- OLE links, tracking 121

- OMID *See* On-media identifiers
 - Online UPS 488
 - On-media identifiers (OMIDs) 58
 - On-site storage, backup media 500
 - Open files counter 411
 - Open requests, NTFS volumes 85 – 86
 - Open searches counter 412
 - Operating system, choosing from NTLDR 619 – 621
 - Operator requests, Removable Storage 57, 66, 76
 - Optical media, moving among media pools 74
 - Optimizing
 - cache usage 322
 - memory 296 – 297, 300
 - multiprocessor installations 438 – 443
 - paging files 297 – 300
 - performance, application design 443 – 445
 - Original disks, mirrored volume failures 482
 - Orphans
 - partitions 547
 - printers, pruning 206 – 207
 - OS/2, printing from 191 – 193
 - OSI layers 397
 - Out-of-date files, Stop 0x79 message 659
 - Output destination rules, 16-bit applications 192 – 193
 - Output Queue Length counter 399
 - Output redirection
 - LPR utility 194
 - NetWare clients 199
 - Overhead
 - controlling performance monitoring 272
 - converting FAT volumes to NTFS 156
 - frequent processor monitoring 331
 - protocol headers and transmission rates 397
 - Overlocking CPUs, Stop 0x7F message 667
- P**
- Packets 414, 580
 - Packets Outbound Discarded counter 399
 - Page Fault Monitor (Pfmon.exe) 308
 - Page faults 291, 306 – 310
 - Page Faults Delta measure 254
 - Page Faults measure 254
 - Page file, RAID-5 volumes 482
 - PAGE_FAULT_IN_NONPAGED_AREA Stop message 655 – 656
 - Paged Pool measure 254
 - Paged pools 293
 - Pages/sec counter 263
 - Paging file *See* Memory
 - Paging File object 229
 - Parallel ports (LPTs), detecting print devices on 180
 - Parity random access memory (RAM) 486
 - Parity strips 477
 - Partition boot sector file 125
 - Partition tables
 - description 12
 - extended boot record (EBR) 19 – 21
 - fields 12 – 19
 - size limitations of 137
 - Partitioning
 - deferred procedure calls (DPCs) 440 – 442
 - full 438
 - hardware interrupt 442
 - threads 439 – 440
 - Partitions
 - active 617
 - basic disks 8
 - boot 475
 - dynamic disks 471
 - mirroring 475
 - orphaning 547
 - restoring configurations 546
 - setting, Fdisk command 39
 - starting sectors 15
 - Stop 0x7B message 663
 - system 475
 - troubleshooting 6
 - upgrading to dynamic disks 7
 - walking 10
 - Password, Recovery Console 529
 - PathPing tool 580
 - Pattern Match Then Buffer Space trigger 420
 - Pattern Match trigger 420
 - Peak committed memory 301
 - Peak Memory Usage measure 254
 - Peer Web Services 173
 - Peer-to-peer networks 163
 - Perfmon4.exe 234
 - Perfmtr.exe 258, 289
 - Performance
 - application 443 – 445
 - FAT16, FAT32, and NTFS speed 135
 - file and folder compression 147
 - monitoring
 - analyzing results of 261 – 264
 - baseline, establishing 261, 277
 - counters 230 – 232

Performance (*continued*)monitoring (*continued*)

data collection architecture 226 – 232

definitions of terms used in 225 – 226

disks *See* Disks

event tracing 231

instances 230 – 231

investigating bottlenecks 265 – 266

legacy applications 278 – 282

network printers 213 – 219

networks 393 – 428

overhead 272

Performance Logs and Alerts tool *See* Performance
Logs and Alertsperformance object minimum configuration 258 –
261

performance object thresholds 263 – 264

performance objects 227 – 230

processors *See* Processors, monitoring

queues, description 226

remote computers 272 – 275

response time, description 226

scheduling data collection 231

servers 275 – 278

SMP systems *See* symmetric multiprocessing

throughput, description 226

tools for 232 – 258

troubleshooting 267 – 272

using System Monitor *See* System Monitor
using Task Manager *See* Task Manager

striped volumes 473

Performance baseline 398

Performance Console 232, 233

Performance Counter 515

Performance Logs and Alerts

creating logs and alerts 245 – 248

exporting log data 249

log file names 249

log file size 249

monitoring performance with 243 – 249

recording transient data 249

sample settings file 245

starting 244 – 245

starting or stopping logs and alerts 249

starting Performance Console 232 – 233

trace data providers 249

trace logs 413

troubleshooting logs 270 – 271

Performance Monitor

checking nonpaged pools for memory leaks 312

description 258

evaluating memory and cache usage 289 – 323

monitoring thread and process priorities 357

Performance Options dialog box 359

Permissions

backup and restore 499

backup and restore operations 499 – 500

CacIs tool 152

inheritable 138

moved and copied files 139

setting

FAT volumes 140

Macintosh clients 202

NTFS volumes 138

share permissions 138, 140

Personal Online Support 566

Pfmmon.exe *See* Page Fault Monitor (Pfmmon.exe)

Phase 0 initialization Stop messages 642

Phase 1 initialization Stop messages 642

Physical Drive Number field 27 – 31

Physical layer 397

Physical media 52

Physical Memory counter 257

PhysicalDisk object

counters 371 – 373

description 229, 370 – 371

Physically full Remote Storage 90

PID measure *See* Process Identifier measurePjilmon.dll *See* Printer Job LanguagePJL *See* Printer Job Language

Placeholders

deleting 86

moving and copying 86 – 87, 88

opening 85 – 86, 98, 99

premigrated files as 79

renaming 80, 86 – 87

restoring 87

volume mount points and symbolic links 88

Planning

backups 501 – 511

configurations

avoiding single points of failure 485 – 491

contingency planning, system recovery 454 – 456

data recovery and restoration 454

developing system recovery plans 459 – 461

fault-tolerant disks 465 – 485

hardware and software upgrades 453 – 454

Planning (*continued*)configurations (*continued*)

- maintaining configuration and system information 457

- security 453

- system maintenance 452 – 453

- top-down and bottom-up execution 452

- training personnel for system recovery 462

- for troubleshooting problems 605

Plotter devices 171

Plug and Play devices

- default settings 574

- installing local printers 180

- Plug and Play specification 603

- print devices 180

pmon.exe *See* Process Monitor (pmon.exe)

Pool memory 651

Pool Monitor (Poolmon.exe) 316

Pool Nonpaged Bytes counter 254, 257

Pool Nonpaged Failures counter 408

Pool Nonpaged Peak counter 408

Pool Paged Bytes counter 254, 257

Pool Paged Failures counter 409

Pool Paged Peak counter 409

Pool tags 316

Pooling printers 161

Poolmon.exe (Pool Monitor) 316

Pools

- creating in Removable Storage 557

- nonpaged

- description 293

- memory leaks 312 – 313

- Stop 0x77 message 658

- Stop 0x7A message 661

- paged 293

- Removable Storage and 55 – 56

Port monitors

- See also* Monitors

- overview 177 – 178

- preferred types for Windows 2000 162

- Sfmmon, printing documents from 203

Portable computers

- dynamic disk support 9

- troubleshooting problems 613

Ports

- administering remotely 178

- choosing 177

- FILE 177

- Hpmon 190 – 191

Ports (*continued*)

- IE, in libraries 54

- IrDA (Infrared) ports 180

- LPT, detecting print devices on 180

- NUL, testing client connectivity with 177

POSIX 140 – 141

POST *See* Power-On Self Test routine

PostScript

- binary jobs 202

- troubleshooting scanner output 197

PostScript Printer Driver (PPD) 170 – 171, 197

Power supply, UPC 486 – 488

Power-On Self Test (POST) routine 616

PPD *See* PostScript Printer Driver

Premigrated files

- converted to placeholders 79

- deleting 86

- premigration schedule 83

- read, write, and memory map requests 85

- renaming, moving, and copying 80, 107

- system files excluded 83

- truncated 82, 83 – 84

Presentation layer 397

Print jobs 161

Print monitors 176 – 178

Print processors 175 – 176

Print Queue object 229

Print Server for Macintosh 200 – 202

Print servers

- Active Directory sites

- Computer object 205, 206

- directory service integration 204 – 205

- Group Policy settings 208 – 209

- non-Windows 2000 printers 208

- printer location tracking 209

- printQueue object 205

- publishing printers 205 – 207

- site topology 204

- sites without domain controllers 207

- description 162

- forwarding print jobs 181

- HP Network Print Monitor (Hpmon) 190 – 191

- Internet printing 185 – 189

- NetWare 199

- network architecture 162 – 165

- non-Windows 2000 clients

- AppleTalk protocol 203

- LPR/LPD utility 193 – 198

- Macintosh clients 200 – 203

Print servers (*continued*)non-Windows 2000 clients (*continued*)

- MS-DOS clients 191 – 193
- NetWare clients 198 – 200
- OS/2 clients 191 – 193
- UNIX clients 193 – 198
- Windows 3.1 clients 191 – 193
- Windows 95 clients 191
- Windows 98 clients 191

print router 172

print server services 172 – 173

printing process 166

remote print provider 171 – 172

remote printing 181

spooler 173 – 175

URLs 185 – 186

Print Services for Unix

default data types 194 – 195

installing 193

purpose of 173

Printcap files 196

Printer drivers

16-bit applications 169

description 161, 169 – 170

Graphical Device Interface (GDI) 169

HP-GL/2 Plotter Driver 171

included with Windows 2000 169 – 171

print processors 175

Universal Printer Driver (Unidriver) 170

viewing in Computer Management snap-in 567 – 570

Windows 2000 PostScript driver 170 – 171, 197

Printer Job Language (PJM) 176

Printer pooling 161

Printer Pruning policy setting 208

Printers

Active Directory directory service

default print behavior 205

Group Policy settings 208 – 209

non-Windows 2000 printers 208

printer location tracking 209

printer searches 191

pruning orphans 206 – 207

publishing printers 205 – 207

Windows 2000 print subsystem 204

auditing events 214 – 216

bi-directional printing 176

Cluster service 210 – 213

connecting to 165

Printers (*continued*)

device drivers *See* Printer drivers

Hardware Compatibility List 169

installing

Add Printer Wizard 165, 178 – 180

from Web page 166, 186 – 187

in clusters 212

unattended setup 217 – 218

logical 161

monitoring performance 213 – 219

network architecture 166 – 178

non-Windows 2000 operating systems 191 – 203

overview 161 – 166

Plug and Play 180

scripts 218 – 216

sharing 178 – 191

spooler

auditing events 216 – 217

client 171

server 173 – 175

Printing System Monitor data 241

Priority Base counter 252, 328, 329

Priority classes, thread 329, 354 – 355

Priority Current counter 329

Priority inversion 356

Private Bytes counter 255

Privileged mode

graphing processor time in 256

processes and threads 349 – 350

PrtAdmin tool 218 – 219

Probabilities of failure, assessing 455

Process Identifier (PID) measure 255

Process Monitor (pmon.exe) 313

Process object

description 229

monitoring memory 304, 311 – 312

monitoring nonpaged pool space 312 – 313

monitoring processor activity 328, 331

Task Manager Process measures 252 – 255

Process Viewer (Pviewer.exe) 350, 359

Processes

changing priorities 358 – 360

finding number of threads in 345 – 347

in user mode or privileged mode 349 – 350

monitoring 340

monitoring priorities 357

priority classes 329

process identifiers 329

process throttling 329

Processes (continued)

- Process Viewer utility 350, 359
- Processes counter 257
- processor bottlenecks 340 – 344
- thread context switches 348 – 349
- tracking processor usage per thread 347 – 348
- viewing running processes 251 – 255

Processor object counters 328, 331

Processor Queue Length counter

- description 328
- monitoring 334 – 337
- recommended threshold 264

Processor Time counter 333 – 334

Processor\% Processor Time counter 434 – 435

Processors

- adding 443
- bottlenecks
 - analyzing counter values 332
 - common causes 332
 - context switches 338 – 339
 - eliminating 362 – 363
 - improving CPU response time 332 – 333
 - monitoring interrupts 337 – 338
 - monitoring threads 345
 - privileged mode 349 – 350
 - process consumption 340 – 344
- Process Viewer utility 350
- processor queue length 334 – 337
- Processor Time counter 333 – 334
- processor-intensive workloads 341 – 342
- thread context switches 348 – 349
- user mode 349 – 350
- monitoring
 - establishing baselines 330 – 331
 - Idle process 330
 - overview 325 – 327
 - process monitoring in Task Manager 251 – 255
 - processor counters 260, 328 – 329
 - Resource Kit tools 330
- print 175 – 176
- process throttling 329
- RIP 201
- symmetric multiprocessing (SMP)
 - application design and 443 – 444
 - monitoring activity 433 – 438
 - Network Load Balancing and scaling 445 – 446
 - optimizing and tuning installations 438 – 443
 - overview 431 – 433

Processors (continued)

- thread priority
 - monitoring thread dispatch states 351 – 353
 - priority classes 354 – 355
 - testing 360 – 362
 - thread scheduling 355 – 356
 - tools for 356 – 360
- upgrading 443
- Product Support Services
 - information to gather before contacting 605
 - questions used to analyze symptoms of problems 600
 - sending Memory.dmp files to 598
- Profiling applications 342
- Programs *See* Applications
- Programs menu, adding Administrative Tools menu 233
- Project Ascent 565
- Promiscuous mode 415
- Properties
 - description 422
 - protocol
 - description 423
 - System Monitor
 - ActiveX control 287 – 288
 - colors 240
 - data 240
 - fonts 240
 - general 240
 - graph 241
 - Source 241
- Properties option 239
- Property filter item 422
- Protecting boot sectors 33
- Protecting Remote Storage data 100 – 101, 521 – 522
- Protocol filter item 422
- Protocol header overhead, effect on transmission rates 397
- Protocols
 - AppleTalk 420
 - DHCP, troubleshooting 610
 - frames sent by specific, viewing 423
 - LPR, remote printing 182 – 183
 - NetBEUI 420
 - NWLink 404
 - originating from specific computers, viewing 423
 - properties 423
 - Raw, remote printing 182 – 183

Protocols (*continued*)

SNMP and SPM 185

TCP/IP *See* TCP/IP

Providers

local print servers 173 – 175

Nwprovau, print processing 200

remote print clients 171 – 172

Pruning Interval policy setting 208

Pruning orphans, printers 206 – 207

Pruning Retries policy setting 208

PSCRIPT1 data type, Print Server for Macintosh 201

Publishing Windows 2000 printers 205 – 207

Pubprn.vbs 208

Pviewer.exe *See* Process Viewer**Q**

Qslice tool 330

Quantums, scheduling threads 355

Querying available disk space 121

Queue Length counter 264, 410

Queue length, monitoring 435 – 436

Queued state 57

Quota disabled state 105

Quota tab 103

Quota tracked state 105

Quota, disk *See* Disk quotas

Quotation marks in long file names 127 – 128

R

RAID arrays 467

RAID-5 volumes

advantages of 478

compared to mirrored volumes 475

creating 15, 479, 480

deleting 551

disadvantages of 478 – 479

disk reads and writes 380

mass storage configurations 482 – 484

moving between Disk Groups 469 – 470

page file location 482

recovering 547, 550 – 551

replacing stripes 550

resolving disk bottlenecks with 389

structure 476 – 478

viewing status in Disk Management 465 – 467

Random access memory (RAM)

4-GB RAM Tuning option (4GT) 300

error-corrective coding (ECC) 486

failure 661

nonparity 487

parity 486

RAID-5 volumes 479

setting Windows RAM usage 628

Random data access 391

Raster driver *See* Universal Printer Driver

Raster image processors (RIP) 201

RAW data type

print processors 175

Print Server for Macintosh 201

printer server service 172

Raw protocol, remote printing 182 – 183

Rd command, Recovery Console 537

Read failures, mirrored volumes 474

Read map requests, NTFS files 85

Reads

orphaning partitions 547

random data access 391

speed of in Windows 2000 135

testing 379 – 380

Reads Denied/sec counter 407

Real Time class 354

Recall notification, Remote Storage 92, 97

Recalling unnamed data attributes 80

Reconfiguring TCP/IP ports 184

Recordkeeping for troubleshooting 596

Records, file and directory 125

Recoverability in NTFS 133

Recovering

disk configurations 546

encrypted files 518

mirrored volumes 476, 547 – 549

NTFS data 148 – 149

placeholders 87

RAID-5 volumes 476, 547, 550 – 551

recovery and restoration planning 454, 459 – 462

Remote Storage data 100 – 101, 551 – 559

Remote Storage database 552, 554 – 556

Removable Storage databases 71 – 72, 552 – 554

restoring data from backups *See* Backups, restoring

Recovery Console

commands 531 – 538

password 529

recreating Boot.ini 540

repairing damaged MBRs and boot sectors 39 – 41

- Recovery Console (*continued*)
 - repairing Windows 2000 installations 527 – 530
 - replacing registry 540
 - Setup floppy disks 462
 - troubleshooting Windows 2000 startup 633 – 634
- Recreating master media 558
- Redirecting printing
 - for printing from Windows 3.x, MS-DOS, and OS/2 192
 - output destination rules 192 – 193
- Redirecting screen output, IPConfig tool 578
- Redirector object 229, 406
- Redo information 149
- Reduction in cache size 320
- Redundant array of independent disks (RAID) *See* Fault-tolerant systems
- Redundant array of independent disks level 5 (RAID-5) *See* RAID-5 volumes
- Reference libraries, creating 457
- Reference points *See* Baselines
- Refresh Active 588
- Refresh All 588
- Refused state 57
- Registration databases, backing up 515
- Registry
 - backups
 - backing up registry 540, 515
 - restoring 544 – 545
 - Emergency Repair Disk (ERD) 541
 - memory management settings 294 – 296
 - registry editors 587 – 589
 - Remote Registry Service 274
 - structure 586 – 587
 - subkeys, monitoring network connections with 403
 - TCP/IP entries 402
 - troubleshooting 589 – 595
- Reinstalling Windows 2000 543
- Relative Sectors field, partition tables 18 – 19, 21
- Reliability, striped volumes 473
- Remote backups 497
- Remote computers
 - backing up files 520
 - enabling disk quotas on 106
 - monitoring 272 – 275
- Remote control programs, Stop message 649
- Remote port monitors 178
- Remote ports, administering 178
- Remote print providers 171 – 172
- Remote printing
 - installing print shares 181
 - overview 162 – 165
 - redirectors 192
- Remote Registry Service 274
- Remote Storage
 - backing up files 519
 - Disk Management attribute 82 – 83
 - managing data storage 49, 78 – 101
 - monitoring disk space with 374
 - recovering data 551 – 559
 - removable media 90
 - reparse points 150
 - restoring database 552, 554 – 556
- Remote Storage Engine 88 – 90
- Removable Storage
 - backups 516
 - creating pools 557
 - managing data storage 47 – 48, 50 – 78
 - restoring databases 552 – 554
 - troubleshooting 77 – 78
- Ren command, Recovery Console 537
- Rename command, Recovery Console 537
- Renaming
 - files on FAT volumes 116 – 117
 - placeholders 86 – 87
 - placeholders and premigrated files 80
 - premigrated files 86 – 87
- Reparse Point attribute type 126
- Reparse points
 - changing into placeholders 88
 - description 119, 150
 - Remote Storage 150
 - reparse attribute 150
 - using in Windows NT 122, 123
- Repartitioning errors, Stop 0x7B message 663
- Replacement costs, estimating 456
- Replicating
 - files 88
- Reports, System Monitor 236, 241
- Requests, I/O 391 – 392
- Reserved field 27 – 31, 29
- Reserved memory 293
- Reserved Sectors field 25 – 29
- Reserved state 61
- Resets, causes of 424
- Resetting statistics 418
- Resource connections counter 411
- Resource settings, changing 574

Response time 226, 332
 Respooling, LPR utility 197
 Restarts, forcing for printers 207
 Restoration planning, data 454
 Restoring damaged data *See* Recovering
 Restoring data from backups *See* Backups, restoring
 Restricting log size 249
 Resynchronizing mirrored volumes 549
 Rewritable media, moving among media pools 74
 Rmdir command, Recovery Console 537
 Robotic libraries 54, 69
 Root Cluster Number field 29
 Root Entries field 25 – 29
 Root file name index 125
 Root folders
 FAT16 volumes 113
 spooling to 174
 Rotating media 100
 Routers, disrupted network connections 490 – 491
 Routing print documents 172
 RsTore.exe 552
 Runaway recalls 86
 Rundll32 command 217
 Running command files during power failures 489
 Running processes, viewing 251 – 255

S

Sabotages, data recovery planning 454, 454
 Safe mode 629 – 633, 653
 SAM registry key 589
 Save As option 239
 Scale factor 431
 Scaling
 benefits of 431
 FAT volumes 116
 network load 445 – 446
 Scandisk 658, 661, 664
 Scanners 197, 647
 Scheduled File Truncation, Remote Storage 84
 Scheduling
 backup 505 – 506
 monitoring with log services 331
 threads 336, 355 – 356
 Screen output, redirecting with IPConfig tool 578
 Screen savers, processor time 341
 Scripting in Removable Storage 77
 Scripts, logon 518 – 519
 Scripts, printer 218

SCSI *See* Small computer system interface
 Scsi() syntax, Boot.ini 617
 Searches, closing in MS-DOS 420
 SecondLevelDataCache registry entry 297
 Sector field 15 – 18
 Sector Per Track field 25 – 29
 Sectors
 512-byte, maximum cluster size 17
 boot *See* Boot sector
 critical to startup 10 – 33
 formatting multiple-boot configurations 134
 size limitations 137
 Sectors Per Cluster field 25 – 29
 Sectors Per FAT field 25 – 29
 Security
 access control lists 67, 152 – 153
 access permissions 138 – 140
 backups 498 – 501, 509
 installing printers from Internet 187 – 189
 Macintosh clients 202
 monitoring remote computers 274 – 275
 planning 453
 Remote Storage support 88
 Security Configuration and Analysis snap-in 538
 Security Descriptor attribute type 126
 Security file 125
 Security log 583
 SECURITY registry key 589
 Seek operation 391
 Select registry subkey 593
 Sequencing, TCP 424
 Sequential data access 391
 Server Announce Allocations Failed/sec counter 405
 Server Message Block (SMB) 424
 Server object 230, 407 – 409
 Server Service, troubleshooting 410 – 412
 Server Sessions Hung counter 407
 Server Work Queues object 230, 409 – 412
 Server Work Queues\Queue Length counter 337
 Server-only backups 496 – 497
 Servers
 counters for establishing baselines for disk usage 382
 monitoring 275 – 278
 NetWare, printing from 198 – 200
 print 217
 Print for Macintosh 200 – 202
 recommended counter thresholds for 264
 running remote backups 497

- Servers (*continued*)
 - spoolers, network printers 173
 - Unix, printing from 193 – 198
 - Windows 2000 memory recommendations 292
- Service packs
 - checking version 648
 - downloading from Windows Update 577
- ServiceGroupOrder registry subkey 594 – 595
- Services
 - Active Directory Replicator, logon scripts 519
 - Browser, troubleshooting performance 405 – 406
 - certificate, backing up 514
 - Client, printing documents 199 – 200
 - Cluster, printing with 210 – 213
 - Component, backing up registration databases 515
 - Exchange, backing up and restoring 522 – 523
 - File and Print for NetWare, printing 198 – 199
 - Gateway, printing 199 – 200
 - link-tracking 121
 - loaded at startup 625
 - Log File, redo and undo information 149
 - log, scheduling monitoring with 331
 - memory consumption 301, 302
 - monitoring 275 – 278
 - Print for Unix 193
 - print server 172 – 173
 - Server, troubleshooting performance 410 – 412
 - Srv.sys 172
 - stopping 340
 - system
 - Stop 0x1E message 649
 - Stop 0x50 message 655
 - Stop 0xC000021A message 668
 - Stop message 647
 - troubleshooting 611 – 612
 - Windows 2000 UPS 489
 - Windows 2000, backing up features 520
- Services for Macintosh volumes, Stop message 651
- Services registry subkey 594 – 595
- Session layer 397
- Session Stats pane 417
- Sessions Errored Out counter 409
- Set Affinity command 439
- SET parameters, displaying 538
- Setup
 - disk set for Windows 2000 462
 - Remote Storage 95
 - troubleshooting 608
- Setup.log 541
- SFC *See* System File Checker tool
- Sfmmon port monitor 203
- Sfmprprt.dll 175
- Share permissions 138, 140
- Shared nothing 446
- Shares, Dfs 374
- Sharing
 - libraries with external applications 91
 - network printers 178 – 191
- Shelf media, Remote Storage 90
- Shells, integration with Remote Storage 94
- Short file names 128 – 129
- Showperf.exe 258
- Side states, Removable Storage 61
- Sides
 - allocation of in media 64
 - state transitions and 62
 - unrecognized 63
- Signature files, antivirus programs 575
- Signature files, updating 37
- Signature words 21
- Signed system files, verifying 573
- Simple Network Management Protocol (SNMP) 185
- Simplifying graphs, System Monitor 242
- Single points of failure, avoiding 485 – 491
- Single processors, mixing files 659 – 660
- Single tape libraries, Remote Storage 78
- Single-threaded applications, adding processors 342
- Size
 - clusters
 - changing, FAT16 volumes 112
 - compression limitations, NTFS 141
 - decreasing, FAT32 volumes 115
 - NTFS volumes 123
 - file system cache 293 – 295, 320
 - files, FAT32 volumes 115
 - I/O requests 391 – 392
 - logs, limiting 249
 - maximum for volumes
 - FAT16 136
 - FAT32 136 – 137
 - NTFS 137
 - paging files, setting 298 – 300
- Skipping files during backups 517 – 518
- Slots in libraries 53
- Slow links, improving performance over 402 – 403
- Small computer system interface (SCSI)
 - adapter errors 43, 647, 663
 - cables, troubleshooting 607

Small computer system interface (SCSI) *(continued)*

- controllers, setting translation mode 480
- corrupt drivers 650, 661, 663
- devices, troubleshooting 607
- multiple controllers in mirrored volumes 481
- signature() Boot.ini entry 617 – 618
- Stop messages
 - Stop 0x24 message 650
 - Stop 0x7A message 661
 - Stop 0x7B message 663
- Small Sectors field 25 – 29
- SMB *See* Server Message Block
- SNMP (Simple Network Management Protocol) 185
- Soft processor affinity 439
- Software *See* Applications
- Software interrupt *See* Deferred procedure calls
- SOFTWARE registry key 589
- Software traps, Stop messages 644
- Sorting events 583
- Sorting items in legends, System Monitor 241
- Source property, System Monitor 241
- Spanned volumes 22, 471 – 472
- Sparse files
 - NTFS support 119 – 120
 - using in Windows NT 122, 123
- Spikes
 - establishing baselines for disk usage and 384
 - excluding from baselines 331
- Split IO/sec counter 373
- SPM *See* Standard TCP/IP Port Monitor
- Spool folders 174
- Spoolers
 - client, network printers 171
 - creating 210 – 211
 - failovers 213
 - logging events 216 – 217
 - LPR utility 197
 - server, network printers 173
- Spreadsheets
 - exporting logs to 249
 - inserting System Monitor ActiveX control 283 – 286
- Standalone drives 54
- Standalone printers 163
- Standard Information file attribute type 126
- Standard TCP/IP Port Monitor (SPM) 181 – 186
- Standby UPS 488
- Start command, changing priority classes 359
- Start registry entry 595
- Starting Cylinder field 15 – 18

Startup

- boot sectors and 22 – 23
- Boot.ini file *See* Boot.ini
- bootstrap loader process 617 – 618
- detecting hardware 622
- disk sectors critical to 10 – 33
- Emergency Repair Disk (ERD) 634 – 635
- initial startup process 616
- LastKnownGood configuration 591 – 592
- loading kernels 623 – 625
- loading operating system 619 – 622
- log on 625
- Power-On Self Test (POST) routine 616
- Recovery Console 629, 633 – 634
- Removable Storage 68
- restoring startup files 544 – 545
- reverting to Last Known Good Configuration 647
- safe mode 629 – 633
- Setup floppy disk set 462 – 463
- Startup disk
 - active partitions 617
 - floppy disk 464 – 465
- Stop messages 642 – 643
- troubleshooting 625 – 635, 609
- Windows 2000 requirements 615 – 616

State transitions 62 – 63

Station Stats pane 417

Statistics

- displaying, NBTStat tool 580
- resetting 418

Status codes, Stop 0x77 message 657 – 661

Status reporting, LPR utility 198

STATUS_IMAGE_CHECKSUM_MISMATCH Stop message 669 – 672

STATUS_SYSTEM_PROCESS_TERMINATED Stop message 668 – 669

Stop 0x0000000A message 646 – 648

Stop 0x0000001E message 648 – 650

Stop 0x00000024 message 650 – 652

Stop 0x0000002E message 652 – 654

Stop 0x00000050 message 655 – 656

Stop 0x00000077 message 657 – 659

Stop 0x00000079 message 659 – 660

Stop 0x0000007A message 660 – 662

Stop 0x0000007B message 662 – 664

Stop 0x0000007F message 665 – 667

Stop 0x1E message 648 – 650

Stop 0x24 message 650 – 652

Stop 0x2E message 652 – 654

- Stop 0x50 message 655 – 656
- Stop 0x77 message 657 – 659
- Stop 0x79 message 659 – 660
- Stop 0x7A message 660 – 662
- Stop 0x7B message 41, 662 – 664
- Stop 0x7F message 665 – 667
- Stop 0xA message 646
- Stop 0xC000021A message 668 – 669
- Stop 0xC0000221 message 669 – 672
- Stop Capture trigger 420
- Stop messages
 - at Windows installation 642
 - at Windows startup initialization 642 – 643
 - blue screen messages 637
 - bugcheck information 640
 - caused by software traps 644
 - DATA_BUS_ERROR 652 – 654
 - debug port information section 641
 - diagnosing Stop errors 644 – 646
 - Error and Event Messages Help 584
 - INACCESSIBLE_BOOT_DEVICE 662 – 664
 - IRQL_NOT_LESS_OR_EQUAL 646 – 648
 - KERNEL_DATA_INPAGE_ERROR 660 – 662
 - KERNEL_STACK_INPAGE_ERROR 657 – 659
 - KMODE_EXCEPTION_NOT_HANDLED 648 – 650
 - MISMATCHED_HAL 659 – 660
 - NTFS_FILE_SYSTEM 650 – 652
 - occurrence of 639
 - overview 581 – 582, 639 – 640
 - PAGE_FAULT_IN_NONPAGED_AREA 655 – 656
 - parts of 640
 - recommended action section 641
 - STATUS_IMAGE_CHECKSUM_MISMATCH 669 – 672
 - STATUS_SYSTEM_PROCESS_TERMINATED 668 – 669
 - Stop 0x0000000A 646 – 648
 - Stop 0x0000001E 648 – 650
 - Stop 0x00000024 650 – 652
 - Stop 0x0000002E 652 – 654
 - Stop 0x00000050 655 – 656
 - Stop 0x00000077 657 – 659
 - Stop 0x00000079 659 – 660
 - Stop 0x0000007A 660 – 662
 - Stop 0x0000007B 662 – 664
 - Stop 0x0000007F 665 – 667
 - Stop 0x1E 648 – 650
 - Stop 0x24 650 – 652
- Stop messages (*continued*)
 - Stop 0x2E 652 – 654
 - Stop 0x50 655 – 656
 - Stop 0x77 657 – 659
 - Stop 0x79 659 – 660
 - Stop 0x7A 660 – 662
 - Stop 0x7B 662 – 664
 - Stop 0x7F 665 – 667
 - Stop 0xA 646
 - Stop 0xC000021A 668 – 669
 - Stop 0xC0000221 669 – 672
 - troubleshooting 672
 - types of 639, 641
 - UNEXPECTED_KERNEL_MODE_TRAP 665 – 667
 - writing memory dump files 482
 - writing to Memory.dmp 598
- Storage devices 495 – 496
- Storage pools 89
- Storage, data *See* Managing data storage
- Storing backup media 500 – 501
- Streams, data 414
- Streams, named 107
- Strings, %systemroot% 616
- Striped volumes
 - disk reads and writes 380
 - overview 472 – 473
 - resolving disk bottlenecks with 389
 - starting Windows 2000 from 22
- Subkeys, registry 403
- Submitted state 57
- Subtrees, Registry 587
- Success Audit events 583
- Summary pane 421
- Swap files *See* Memory, paging files
- Switching between adapters 420
- Symbolic links, changing into placeholders 88
- Symmetric interrupt distribution 442
- Symmetric multiprocessing (SMP)
 - application design and 443 – 444
 - monitoring activity 433 – 438
 - Network Load Balancing and scaling 445 – 446
 - optimizing and tuning installations 438 – 443
 - overview 431 – 433
- Symmetric multiprocessing (SMP) performance
 - monitoring activity 433 – 438
 - Network Load Balancing and scaling 445 – 446
 - optimizing and tuning installations 438 – 443

Symmetric multiprocessing (SMP) performance *(continued)*
 optimizing applications 443 – 445
 overview 431 – 433

Synchronizing restored database files 72

System checklists 599

System File Checker (SFC) tool 575 – 576, 611

System files
 backing up 514
 mismatches, Stop 0xC000021A message 669
 restoring previous version 573
 verifying signature 573
 version checking 575 – 576

System ID field 14 – 15

System Information tool 567 – 573

System log 582

System messages 639

System Monitor
 cache and memory counters 318 – 321
 compared with Task Manager 250
 counterparts to Task Manager counts 256 – 257
 displaying percentages above 100% 232
 Idle process calculations 330
 monitoring 16-bit applications 279 – 281
 monitoring memory leaks 312 – 313
 monitoring network activity
 Application-Layer objects 404 – 409
 NBT Connection object 404
 Network Interface object 399 – 400
 network layer performance objects 397 – 398
 Network Protocol objects 401 – 403
 Network Segment objects 400 – 401
 overview 396 – 398
 Server Work Queues object 409 – 412
 monitoring printer performance 213
 overview 233 – 234
 printing data 241
 Processor Queue Length counter 334 – 337
 setting display options 236 – 241
 starting 234 – 235
 starting Performance Console 232 – 233
 System Monitor ActiveX control
 formatting 286 – 288
 inserting in documents 282 – 285
 inserting in Visual Basic programs 286
 inserting in Web pages 283, 286
 tips for using effectively 241 – 242
 troubleshooting 267 – 272
 using 235 – 243

System object 230

System partitions
 description 475
 formatting 134

System patches, uninstalling 577

System pools 55 – 56

SYSTEM registry key 589 – 591

System services
 Stop 0x1E message 649
 Stop 0x50 message 655
 Stop 0xC000021A message 668
 Stop message 647

System state data
 backing up 511 – 515
 restoring 544

System Summary category, System Information tool 568

System volumes, extending 7

System\Interrupts/sec counter 332

System\Processor Queue Length counter 334 – 337, 435 – 436

Systemroot command, Recovery Console 538

T

Tapes

See also Media

- cleaning drives 75
- moving among media pools 74
- moving to application pools 72
- protecting with media copies 100
- recovering backups 558 – 559
- sides of 52

Task Manager

- checking installed memory 293
- checking virtual memory 301
- compared with System Monitor 250
- description 232
- monitoring 16-bit applications 280 – 281
- monitoring processes
 bypassing I/O counts 369
 changing base priorities 358
 Idle process calculations 330
 Processes tab 251 – 255
- monitoring system performance 255 – 257
- nonpaged pool size value 312
- Set Affinity command 439
- starting 250
- user interface 250 – 251

- Tasks, delegating 508
- TCP sequencing 424
- TCP/IP
 - IPConfig tool 578
 - NBT Connection object 404
 - NetBIOS name resolution 580
 - NetDiag tool 578
 - Network Interface object 399 – 400
 - Network Segment object 401
 - print servers
 - Cluster service 212
 - installing 162
 - LPD utility 194
 - LPR utility 195
 - NetWare 198
 - Standard TCP/IP Port Monitor (SPM) 181 – 186
 - registry entries 402 – 403, 590
 - trace logs 413
- TcpMaxDataRetransmissions registry subkey 420
- TcpWindowSize registry subkey 420
- Technical reference libraries, creating 457
- Technical support
 - training personnel for system recovery 462
 - troubleshooting Windows 2000 565 – 566
- Telephony object 230
- Testing
 - backup-and-restore procedures 510
 - client connectivity, NUL port 177
 - components causing problems 605
 - data recovery plans 454
 - disk efficiency, preparing for 377 – 378
 - fault-tolerant systems 485
 - priority changes 360 – 362
 - reads and writes 379 – 380
 - recovery procedures 460 – 461
 - system limits, counters recommended for 260
 - throughput 378 – 379
- TEXT data type, print processors 176
- Third-party applications
 - backup programs 546
 - compatibility with Remote Storage 98
 - remote control, Stop 0x1E message 649
 - Stop 0xC000021A message 668
- Thread Count counter 255, 257
- Thread object counters 328 – 329, 331
- Thread priority, changing 349
- Thread scheduling 336
- Thread State counter 328
- Threads
 - bottlenecks, monitoring effects upon 345 – 350
 - changing priority
 - priority classes 354 – 355
 - testing 360 – 362
 - thread dispatch states 351 – 353
 - thread scheduling 355 – 356
 - tools for 356 – 360
 - displayed by Processor Queue Length counter 334
 - finding number of threads in processes 345 – 347
 - Idle process, measuring 330
 - in user mode or privileged mode 349 – 350
 - monitoring 438
 - partitioning 439 – 440
 - scheduling 355 – 356
 - thread context switches 348 – 349
 - tracking processor usage per thread 347 – 348
- Thresholds recommended for counters 263 – 264
- Throughput
 - counters for monitoring 260
 - description 226, 367
 - disks, counters for measuring 371 – 373
 - improving 332
 - testing 378 – 379
- Time response
 - description 226
 - improving 332
- Time slices *See* Quanta
- Time stamp
 - compared to NTFS change journal 119
 - disabling in NTFS 368
 - FAT volumes 114
- Time, tracking processor 340 – 344
- Timeout parameter 619
- Timer bar, System Monitor 235
- Time-sensitive backups 508
- Toolbars, configuring System Monitor with 236
- Tools
 - See also* Applications
 - Application Monitor (ApiMon) 315
 - Autochk 658
 - AVBoot *See* AVBoot tool
 - Backup *See* Backups
 - Cacls 152 – 153
 - Compact 143, 153
 - Compress 154 – 155
 - Convert 155 – 156
 - CPUSTres 330
 - Ctrlist.exe 258

Tools (*continued*)

- Device Manager 574 – 575
- DirectX Diagnostic 572
- DirUse 157
- Disk Cleanup 571
- DiskMap 34
- DiskProbe 10, 34
- DoubleSpace 141, 147
- Dr. Watson 571
- Drivers utility 612
- DriveSpace 141, 147
- Exctrst.exe 258
- Expand 157
- File Signature Verification Utility 573
- FTDisk 102, 474
- IPConfig 578 – 610
- IPSecMon 581
- LeakyApp 300, 314
- LPD and LPR 193 – 198
- Memsnap 313
- Mountvol 158
- NBTStat 580
- NetDiag 578, 610
- Network Connections 572
- Network Monitor *See* Network Monitor
- Page Fault Monitor (Pfmon.exe) 308
- PathPing 580
- Performance console 232 – 234
- Performance Logs and Alerts *See* Performance Logs and Alerts
- Performance Monitor (Perfmtr.exe) *See* Performance Monitor
- performance monitoring 232 – 258, 267
- Pool Monitor (Poolmon.exe) 316
- PnAdmin 218 – 219
- Process Monitor (pmon.exe) 313
- Process Viewer (Pviewer.exe) 350, 359
- Qslice 330
- Recovery Console *See* Recovery Console
- Safe mode 630 – 633
- Scandisk 658, 661, 664
- Showperf.exe 258
- System File Checker 575 – 611
- System Information 567 – 573
- System Monitor *See* System Monitor
- Task Manager *See* Task Manager
- Typeperf.exe 258
- Update Wizard Uninstall 573
- Virtual Address Dump (Vadump) 315

Tools (*continued*)

- Windows Report 573
- Working Set Tuner (WST) 315
- Total Bytes/sec counter 410
- Total Frames Received/second counter 401
- Total Handles count 256
- Total Operations/sec counter 410
- Total Processes count 257
- Total Sectors field 18 – 19
- Total Stats pane 417
- Total Threads count 257
- Trace logs
 - configuring 246
 - file names 249
 - monitoring network performance 413
 - properties 248
 - trace data providers 249
- Tracing events 231
- Tracking file modifications *See* Change journal
- Tracking OLE links 121
- Training personnel for system recovery 462
- Transaction logging and recovery 148 – 149
- Transient data, recording in logs 249
- Translation mode, setting 480
- Transmission Control Protocol/Internet Protocol (TCP/IP) *See* TCP/IP
- Transport layer 397
- Transports
 - description 50
 - in libraries 53
- Traps, bound 665
- Traps, software 644
- Trees, decision 422
- Triggers, for Network Monitor captures 420
- Troubleshooters 585 – 586
- Troubleshooting
 - backups, planning for 508
 - bottlenecks
 - disk 389
 - memory 322 – 323
 - network 425 – 428
 - overview 264 – 266
 - processor 362 – 363
 - Browser Service 405 – 406
 - disks 15, 34 – 43
 - hard page faults 306 – 310
 - memory usage problems 302 – 323
 - partitions 6
 - processor bottlenecks *See* Processors, bottlenecks

Troubleshooting (*continued*)

- Removable Storage 77 – 78
- restored database files 72
- scanner output, Windows 2000 PostScript drivers 197
- Server Service 410 – 412
- Stop messages *See* Stop messages
- video card failures 487
- volumes 6
- Windows 2000 startup 625 – 629
- Windows 2000, general strategies 563 – 613
- with performance tools 267 – 272

Truncation

- placeholders 86 – 87
- premigrated files 86 – 87
- Remote Storage files 83 – 84
- unnamed data attributes 79

Tuning disks

- configuring for optimal performance 367 – 370
- counters 370 – 380
- establishing baselines 381 – 384
- evaluating usage by applications 390 – 392
- investigating problems 385 – 388
- resolving bottlenecks 389

Type command, Recovery Console 537**Type registry entry 595****Typeperf.exe 258****U****UDF (Universal Disk Format) 130****UDP object 230****Unattended setup for printers 217 – 218****Undo information, Log File Service 149****UNEXPECTED_KERNEL_MODE_TRAP Stop message 665 – 667****Unicode, file names 116, 128****Unidriver *See* Universal Printer Driver****Uniform Resource Locator (URL), print jobs 166****Uninstalling device drivers, system patches, and hot fixes 577****Uninterruptible power supplies (UPSs) 486 – 488****Unique Sequence Number (USN) 119****Universal Disk Format (UDF) 130****Universal Printer Driver (Unidriver) 170****Universal Serial Bus (USB)**

- detecting print devices on 180
- publishing Windows 2000 printers 205

Unix

- Portable Operating System Interface (POSIX)
 - compliance 140 – 141
- Print Service for 173
- printing from clients and servers 193 – 198

Unknown volumes, troubleshooting 42**Unloaded state 61****Unnamed data attributes 79, 80****Unprepared state 61****Unrecognized pools 55, 64****Unrecognized state 61****Unsupported disks, Stop 0x7B message 663****Uppercase table file 125****Update Wizard Uninstall tool 573****Updating OLE links 121****Upgrading**

- hardware and software, planning 453 – 454
- network adapters 441
- partitions and volumes to dynamic disks 7
- processors 443
- Remote Storage libraries 90
- servers 278
- Windows, Stop 0xA message 647

UPS *See* Uninterruptible power supplies**USB *See* Universal Serial Bus****User data, backing up on local computers 519****User mode, processes and threads 349 – 350****USER Objects measure 255****User permissions *See* Permissions****USN (Unique Sequence Number) 119****V****Vadump (Virtual Address Dump) 315****Validate Managed Files, Remote Storage 84****Value bars, System Monitor 235****Vendor software failure support 452****Verify Windows 2000 System Files option 543****Version checking, system files 575 – 576****Version compatibility, Remote Storage with third-party remote storage products 98****Video cards, avoiding failures 487****Videos, troubleshooting 610 – 611****Virtual Address Dump (Vadump) 315****Virtual memory**

- description 293
- effects upon RAM consumption 301
- monitoring usage 301

Virtual Memory Manager 305

Virtual Memory Size measure 255
Virus scanners, Stop 0xA message 647
Viruses
 AVBoot antivirus tool *See* AVBoot tool
 backups and 498
 boot sector viruses 35 – 38, 42
 Fdisk command 38
 Master Boot Record viruses 35 – 38
 Remote Storage-aware antivirus programs 99
 Stop 0x77 message 658
 Stop 0x7A message 661
 troubleshooting 604
 updating antivirus programs 575
Visual Basic programs, inserting System Monitor ActiveX control 285
Volume file 125
Volume Information attribute type 126
Volume Label field 27 – 31
Volume mount points
 changing into placeholders 88
 Mountvol tool 158
 overview 150
Volume Name attribute type 126
Volume Serial Number field 27 – 31
Volumes
 basic 6
 boot sectors, running Recovery Console when damaged 528
 configuring and managing, local storage 94
 converting from FAT to NTFS, Convert tool 155 – 156
 creating on dynamic disks 6
 decommissioning 87
 description 150
 dynamic *See* Dynamic volumes
 enumerating 158
 extending 7, 10
 FAT16 *See* FAT16 file system
 FAT16, FAT32, and NTFS speed 135
 FAT32 *See* FAT32 file system
 legacy, Disk Management support 8
 logical 523
 mappings, Recovery Console 530
 maximum sizes
 FAT16 136
 FAT32 136 – 137
 NTFS 137
 mirrored *See* Mirrored volumes
 NTFS *See* NTFS file system

Volumes (*continued*)
 RAID-5 *See* RAID-5 volumes
 restoring configurations 546
 spanned 471 – 472
 spreading paging files across 299
 starting Windows 2000 from 22
 troubleshooting 6
 unknown 42
 upgrading to dynamic disks 7
 Windows NT volume clean-up operations 122 – 123

W

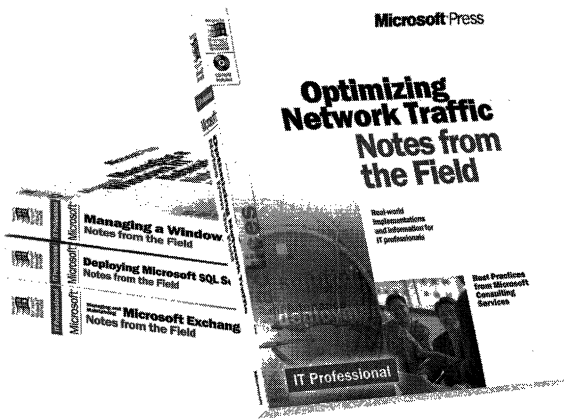
Waiting state 57
Walking partitions 10
WAN *See* Wide area networks
Warning events 583
Warning threshold limit, disk quotas 104
Web pages
 inserting System Monitor ActiveX control 283 – 286
 printing 166 – 189
WFP *See* Windows File Protection
Wide area networks (WANs), slow links 402 – 403
Wildcards
 CacIs tool 152
 deleting and copying files with 128
Win32k.sys
 Stop 0x1E message 649
Windows 2000
 installing
 limitations of dynamic disks when 9
 reinstalling 543
 Stop messages 642, 647
 minimum memory requirement 292
 process priority 359 – 360
 services, backing up features 520
 Setup floppy disk set 462
 startup
 Boot.ini file *See* Boot.ini
 bootstrap loader process 617 – 618
 detecting hardware 622
 Emergency Repair Disk 634 – 635
 initial startup process 616
 LastKnownGood configuration 591 – 592
 loading kernels 623 – 625
 loading operating system 619 – 622
 Power-On Self Test (POST) routine 616
 Recovery Console 629, 633 – 634
 requirements for 615 – 616

- Windows 2000 (*continued*)
 - startup (*continued*)
 - restoring startup files 544 – 545
 - reverting to Last Known Good Configuration 647
 - safe mode 629 – 633
 - Startup floppy disk 464 – 465
 - troubleshooting 625 – 635
 - user log on 625
 - troubleshooting, general strategies for 563 – 613
- Windows 2000 Advanced Server, paging files 300
- Windows 2000 Server Service (Srv.sys) 172
- Windows 2000 shell, integration with Remote Storage 94
- Windows 2000 UPS service 489
- Windows Driver Library (WDL), controller support 663
- Windows Explorer, integration with Remote Storage 93
- Windows File Protection (WFP) 575 – 576
- Windows Frame Viewer 421
- Windows Management Infrastructure (WMI) interface 227
- Windows Network Monitor Capture 417
- Windows Report tool 573
- Windows Update 577
- Wizards
 - Add Port 195 – 196
 - Add Printer 165, 178 – 179, 205
 - Add Standard TCP/IP Port 183 – 184
 - Hardware Wizard 572
 - Update Wizard Uninstall tool 573
- WMI (Windows Management Infrastructure) 227
- Word, placing System Monitor ActiveX control in documents 283 – 286
- Work Item Shortages counter 264, 409 – 410
- Work queues
 - Removable Storage and 56 – 57, 76
 - troubleshooting 78
- Working Set counter, Memory Usage measure 254
- Working Set Tuner (WST) 315
- Workloads, servers 275 – 277
- World Wide Web
 - placing System Monitor ActiveX control into Web pages 283 – 286
 - printing 166 – 189
- Wrappers 399
- Write map requests, NTFS files 85
- Write-back cache, configuring 149
- Writes Denied/sec counter 407
- WST (Working Set Tuner) 315

Z

- Zero idle time 330
- Zero values, troubleshooting 267

There's no ***substitute*** for ***experience.***



Now you can apply the best practices from real-world implementations of Microsoft technologies with NOTES FROM THE FIELD. Based on the extensive field experiences of Microsoft Consulting Services, these valuable technical references outline tried-and-tested solutions you can use in your own company, right now.

Microsoft Press® products are available worldwide wherever quality computer books are sold. For more information, contact your book or computer retailer, software reseller, or local Microsoft Sales Office, or visit our Web site at mspress.microsoft.com. To locate your nearest source for Microsoft Press products, or to order directly, call 1-800-MSPRESS in the U.S. (in Canada, call 1-800-268-2222).

Prices and availability dates are subject to change.

Deploying Microsoft® Office 2000 (Notes from the Field)

U.S.A. \$39.99
U.K. £25.99
Canada \$59.99 [Recommended]
ISBN 0-7356-0727-3

Deploying Microsoft SQL Server 7.0 (Notes from the Field)

U.S.A. \$39.99
U.K. £25.99
Canada \$59.99
ISBN 0-7356-0726-5

Optimizing Network Traffic (Notes from the Field)

U.S.A. \$39.99
U.K. £25.99
Canada \$59.99
ISBN 0-7356-0648-X

Managing a Microsoft Windows NT® Network (Notes from the Field)

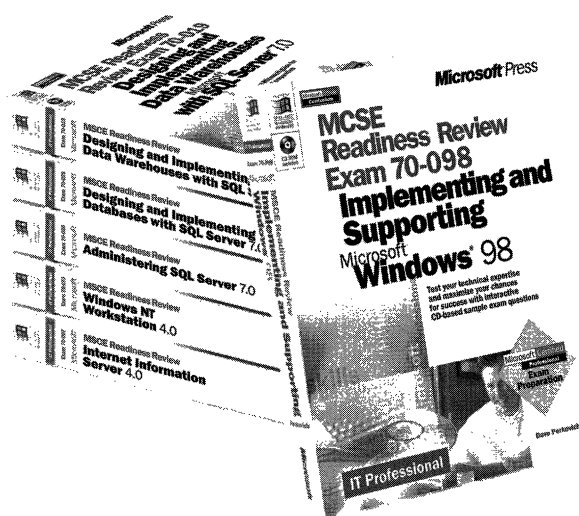
U.S.A. \$39.99
U.K. £25.99
Canada \$59.99
ISBN 0-7356-0647-1

Building an Enterprise Active Directory™ (Notes from the Field)

U.S.A. \$39.99
U.K. £25.99
Canada \$59.99
ISBN 0-7356-0860-1

Microsoft®
mspress.microsoft.com

The **intelligent** way to practice for the **MCP exam**



If you took the Microsoft Certified Professional (MCP) exam today, would you pass? With the *Readiness Review* MCP exam simulation on CD-ROM, you get a low-risk, low-cost way to find out! Use this electronic assessment tool to take randomly generated 60-question practice tests, covering actual MCP objectives. Test and retest with different question sets each time, and then consult the companion study guide to review all featured exam items and identify areas for further study. *Readiness Review*—it's the smart way to prep!

MCSE Readiness Review—Exam 70-058: Networking Essentials

U.S.A. \$29.99
U.K. \$27.99 [V.A.T. included]
Canada \$42.99
ISBN 0-7356-0536-X

MCSE Readiness Review—Exam 70-067: Microsoft® Windows NT® Server 4.0

U.S.A. \$29.99
U.K. \$27.99 [V.A.T. included]
Canada \$42.99
ISBN 0-7356-0538-6

MCSE Readiness Review—Exam 70-073: Microsoft Windows NT Workstation 4.0

U.S.A. \$29.99
U.K. \$27.99 [V.A.T. included]
Canada \$42.99
ISBN 0-7356-0537-8

MCSE Readiness Review—Exam 70-087: Microsoft Internet Information Server 4.0

U.S.A. \$29.99
U.K. \$27.99 [V.A.T. included]
Canada \$44.99
ISBN 0-7356-0541-6

MCSE Readiness Review—Exam 70-098: Implementing and Supporting Microsoft Windows® 98

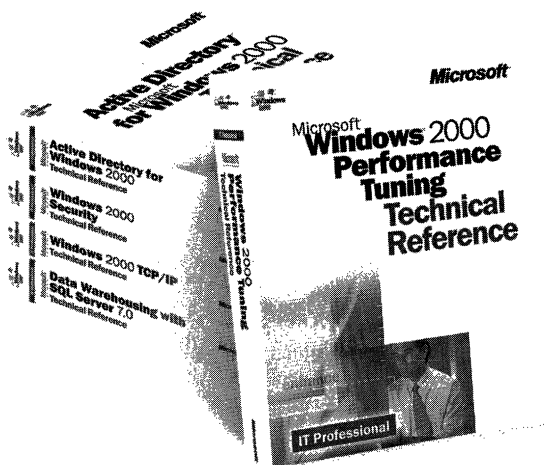
U.S.A. \$29.99
U.K. \$27.99 [V.A.T. included]
Canada \$44.99
ISBN 0-7356-0671-4

Microsoft Press® products are available worldwide wherever quality computer books are sold. For more information, contact your book or computer retailer, software reseller, or local Microsoft Sales Office, or visit our Web site at mspress.microsoft.com. To locate your nearest source for Microsoft Press products, or to order directly, call 1-800-MSPRESS in the U.S. (in Canada, call 1-800-268-2222).

Prices and availability dates are subject to change.

Microsoft®
mspress.microsoft.com

In-depth. Focused. And ready for work.



Get the technical drilldown you need to deploy and support Microsoft products more effectively with the MICROSOFT TECHNICAL REFERENCE series. Each guide focuses on a specific aspect of the technology—weaving in-depth detail with on-the-job scenarios and practical how-to information for the IT professional. Get focused—and take technology to its limits—with MICROSOFT TECHNICAL REFERENCES.

Building Applications with Microsoft® Outlook 2000 Technical Reference

U.S.A. \$49.99
U.K. £32.99 [V.A.T. included]
Canada \$74.99
ISBN 0-7356-0581-5

Active Directory™ Services for Microsoft Windows 2000 Technical Reference

U.S.A. \$49.99
U.K. £32.99
Canada \$76.99
ISBN 0-7356-0624-2

Microsoft Windows NT® 4.0 Security, Audit, and Control Technical Reference

U.S.A. \$49.99
U.K. £32.99
Canada \$71.99
ISBN 1-57231-818-X

Microsoft Windows 2000 Security Technical Reference

U.S.A. \$49.99
U.K. £32.99
Canada \$76.99
ISBN 0-7356-0858-X

Microsoft Windows NT Server 4.0 Terminal Server Edition Technical Reference

U.S.A. \$49.99
U.K. £32.99 [V.A.T. included]
Canada \$74.99
ISBN 0-7356-0645-5

Microsoft Windows 2000 Performance Tuning Technical Reference

U.S.A. \$49.99
U.K. £32.99
Canada \$76.99
ISBN 0-7356-0633-1

Microsoft Windows® 2000 TCP/IP Protocols and Services Technical Reference

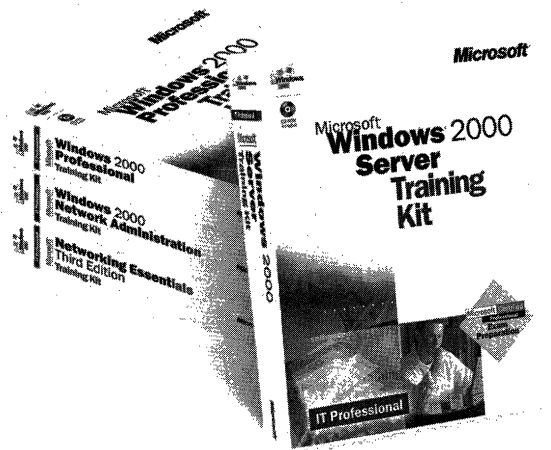
U.S.A. \$49.99
U.K. £32.99 [V.A.T. included]
Canada \$76.99
ISBN 0-7356-0556-4

Microsoft Press® products are available worldwide wherever quality computer books are sold. For more information, contact your book or computer retailer, software reseller, or local Microsoft Sales Office, or visit our Web site at mspress.microsoft.com. To locate your nearest source for Microsoft Press products, or to order directly, call 1-800-MSPRESS in the U.S. (in Canada, call 1-800-268-2222).

Prices and availability dates are subject to change.

Microsoft®
mspress.microsoft.com

Gain work-ready expertise as you prepare for the Microsoft Certified Professional (MCP) exam.



Learn by doing—learn for the job—with official Microsoft self-paced training kits. Whether you choose a book-and-CD TRAINING KIT or the all-multimedia learning experience of an ONLINE TRAINING KIT, you'll gain hands-on experience building essential systems support skills—as you prepare for the corresponding MCP exam. It's Microsoft Official Curriculum—how, when, and where you study best.

Microsoft® Certified Systems Engineer Core Requirements Training Kit
ISBN 1-57231-905-4

Microsoft Windows® 2000 Server Training Kit
ISBN 1-57231-903-8

Microsoft Windows 2000 Server Online Training Kit
ISBN 0-7356-0954-3
COMING SOON

Microsoft Windows 2000 Professional Training Kit
ISBN 1-57231-901-1

Microsoft Windows 2000 Professional Online Training Kit
ISBN 0-7356-0953-5
COMING SOON

Microsoft Windows 2000 Active Directory™ Services Training Kit
ISBN 0-7356-0999-3
COMING SOON

Microsoft Windows 2000 Active Directory Services Online Training Kit
ISBN 0-7356-0994-2
COMING SOON

Microsoft SQL Server™ 7.0 Database Implementation Training Kit
ISBN 1-57231-826-0

Microsoft SQL Server 7.0 Database Implementation Online Training Kit
ISBN 0-7366-0679-X

Microsoft SQL Server 7.0 System Administration Training Kit
ISBN 1-57231-827-9

Microsoft SQL Server 7.0 System Administration Online Training Kit
ISBN 0-7356-0678-1

Networking Essentials, Third Edition
ISBN 1-57231-902-X

Networking Essentials, Third Edition, Online Training Kit
ISBN 0-7356-0880-6

Microsoft Windows 2000 Network Infrastructure Administration Training Kit
ISBN 1-57231-904-6
COMING SOON

Microsoft Windows NT® Network Administration Training
ISBN 1-57231-439-7

Microsoft TCP/IP Training
ISBN 1-57231-623-3

Microsoft Press® products are available worldwide wherever quality computer books are sold. For more information, contact your book or computer retailer, software reseller, or local Microsoft Sales Office, or visit our Web site at mspress.microsoft.com. To locate your nearest source for Microsoft Press products, or to order directly, call 1-800-MSPRESS in the U.S. (in Canada, call 1-800-268-2222).

Prices and availability dates are subject to change.

Microsoft®
mspress.microsoft.com

Microsoft **Windows® 2000 Server** **Operations Guide**

This OPERATIONS GUIDE provides the comprehensive information you need to understand and maintain your Windows 2000 Server-based installations.

Coverage includes:

- Administering Windows 2000 file systems
- Managing removable and remote data storage
- Setting up and configuring network printers
- Evaluating memory and cache usage
- Analyzing processor and multiprocessor activity
- Monitoring network performance
- Backing up and restoring user and system data
- Using troubleshooting tools and strategies