Workstation
Server
Enterprise

CHAPTER

Advanced Troubleshooting Topics

27

About Chapter 27

Chapter 27 explores a number of advanced Windows NT troubleshooting topics.

This chapter begins with a discussion of the Windows NT boot sequence, and recommends solutions to several common boot sequence problems. Included in this section are detailed instructions for performing the Emergency Repair process.

Next, this chapter explains how to use Event Viewer, which can be used to determine why a service or driver failed during system startup. Windows NT Diagnostics, which enables you to view detailed configuration information, is also covered.

Next, this chapter outlines the structure of the Windows NT Registry, and explains how to use the Registry editors to search and modify the Registry.

Various other advanced troubleshooting issues are explored, including diagnosing and interpreting blue screens, configuring a memory dump, configuring Dr. Watson for Windows NT, and configuring a computer for remote debugging.

This chapter includes one comprehensive hands-on lab. You'll get to practice advanced Windows NT troubleshooting techniques, including: using Windows NT Diagnostics, using the Registry editors, configuring a memory dump, and starting and configuring Dr. Watson for Windows NT.

Chapter 27 is a "must read" no matter which of the three Windows NT 4.0 Microsoft Certified Professional exams you're preparing for. This chapter maps to many of the Troubleshooting objectives for these exams.

Troubleshooting the Boot Sequence

The *boot sequence* refers to the process of starting Windows NT, including initializing all of its services and completing the logon process. There are several common problems that can occur during the boot sequence, and in order to successfully troubleshoot them, you need to have an understanding of the steps that occur during the boot sequence.

The following sections identify and explain the steps that occur during the boot sequence, list common boot sequence problems and recommended solutions, and discuss how to perform the Emergency Repair process, which is a solution to several common boot sequence problems.

Overview of the Boot Sequence

The Windows NT boot sequence consists of a sequential series of steps, beginning with powering on the computer and ending with completion of the logon process. Understanding the individual steps that make up the boot sequence will help you to troubleshoot problems that may occur during this process.

The boot sequence steps vary according to the hardware platform you are using. The boot sequence steps discussed in this section apply to the Intel platform only.

The Windows NT boot sequence (Intel platform) is as follows:

1. **Power On Self Test:** The *Power On Self Test* (POST) is performed by the computer's BIOS every time the computer is powered on to test for the existence of specific components, such as processor, RAM, and video adapter. If any errors are detected during this phase, an error message or onscreen diagnostics is typically displayed.
2. **Initial Startup:** In this step, the computer's BIOS attempts to locate a startup disk, such as a floppy disk, or the first hard disk in the computer.

   If the startup disk is the first hard disk, the BIOS reads the *Master Boot Record* from the startup disk, and the code in the Master Boot Record is run. The Master Boot Record then determines which partition is the active partition, and loads sector 0 (also called the partition boot sector) from the active partition into memory. Then the code contained in sector 0 is run. This causes the `Ntldr` file to be loaded into memory from the root folder of the active partition. `Ntldr` is then run.

If the startup disk is a floppy disk, the code from sector 0 on the floppy disk is loaded into memory. Then the code contained in sector 0 is run. This causes `Ntldr` to be loaded into memory from the root folder of the floppy disk. `Ntldr` is then run.

3. **Selecting an operating system:** Ntldr switches the processor into a 32-bit flat memory mode. `Ntldr` then initializes the appropriate minifile system (either FAT or NTFS) to enable `Ntldr` to locate and load the `Boot.ini` file. Ntldr uses the `Boot.ini` file to create the *boot loader screen*.

   A typical Window NT 4.0 boot loader screen appears as follows:

   ```
   OS Loader V4.00

   Please select the operating system to start:

          Windows NT Server Version 4.00
          Windows NT Server Version 4.00 [VGA mode]
          MS-DOS

   Use ↑ and ↓ to move the highlight to your choice.
   Press Enter to choose.

   Seconds until highlighted choice will be started automatically: 30
   ```

   At this point, either the user selects an operating system from the boot loader menu, or the default operating system is automatically started after a specified number of seconds has elapsed.

   If an operating system *other* than Windows NT is selected, the `Bootsect.dos` file is loaded into memory and run, and the appropriate operating system is started. (If an operating system other than Windows NT is selected, the remaining steps of the Windows NT boot sequence do not apply.)

   If Windows NT is selected, Ntldr loads `Ntdetect.com` and executes it.

4. **Detecting hardware:** `Ntdetect.com` searches for computer ID, bus type (ISA, EISA, PCI, or MCA), video adapter, keyboard, serial and parallel ports, floppy disk(s), and pointing device (mouse).

   As it checks, the following is displayed onscreen:

   ```
   NTDETECT V4.0 Checking Hardware . . .
   ```

   `Ntdetect.com` creates a list of the components it finds and passes this information to `Ntldr`.

5. **Selecting hardware profile and loading the kernel:** `Ntldr` displays the following message:

```
OS Loader V4.0
Press spacebar now to invoke Hardware Profile/Last Known Good menu.
```

Ntldr gives you approximately three to five seconds to press the spacebar. If you press the spacebar at this time, the Hardware Profile/Last Known Good menu is displayed as shown:

```
Hardware Profile/Configuration Recovery Menu
This menu enables you to select a hardware profile
to be used when Windows NT is started.

If your system is not starting correctly, then you may switch to a
previous system configuration, which may overcome startup problems.
IMPORTANT: System configuration changes made since the last
successful startup will be discarded.

                Original Configuration
                Some other hardware profile

Use the up and down arrow keys to move the highlight
to the selection you want. Then press Enter.
To switch to the Last Known Good Configuration, press 'L'.
To Exit this menu and restart your computer, press F3.

Seconds until highlighted choice will be started automatically: 5
```

If you press **L** while this screen is displayed, the Last Known Good control set will be used, and any configuration changes made during the last logon session will be discarded.

If you don't press the spacebar and have only one hardware profile, the default hardware profile is loaded.

If you don't press the spacebar and have more than one hardware profile, the Hardware Profile/Configuration Recovery Menu is displayed.

Once you've selected a hardware profile, `Ntldr` loads `Ntoskrnl.exe` and executes the Windows NT kernel.

6. **Kernel initialization:** When the kernel starts, a screen similar to the following is displayed:

   ```
   Microsoft (R) Windows NT (TM) Version 4.0 (Build 1381)
   1 System Processor (32 MB Memory)
   ```

   This screen indicates that the kernel has successfully started.

7. **Initializing device drivers:** At this point, the kernel loads either the default control set or, if you selected the Last Known Good Configuration, it loads the Last Known Good control set. Then the kernel initializes all of the device drivers listed in the control set.

8. **Initializing services:** The kernel loads and starts the services listed in the control set being used.

9. **Logon process:** The Begin Logon dialog box is displayed, prompting the user to press Ctrl + Alt + Delete to log on. Then the user logs on, supplying an appropriate user name and password.

   Once a user has successfully logged on, the boot sequence is complete, and the control set currently in use is copied to the Last Known Good Configuration.

Troubleshooting Common Boot Sequence Problems

There are many common problems that can occur during the Windows NT boot sequence. Table 27-1 lists these problems, along with their possible causes and recommended solutions.

TABLE 27-1 TROUBLESHOOTING THE WINDOWS NT BOOT SEQUENCE

PROBLEM	*POSSIBLE CAUSE*	*RECOMMENDED SOLUTION*
An error message is displayed during the POST.	This message most likely indicates a hardware failure.	Use the error message (or onscreen diagnostics) displayed to determine the offending hardware device. Repair, replace, or reconfigure the hardware device as necessary.

Problem	*Possible Cause*	*Recommended Solution*
An error message, such as "Invalid partition table" or "Missing operating system" is displayed after the POST.	This type of error message often indicates that either sector 0 of the active partition is damaged, or that important operating system files (such as `Ntldr`) are missing.	Perform the Emergency Repair process (as explained in the next section of this chapter) and select the Inspect boot sector option during this process. If you suspect that there are missing files, also select the Verify Windows NT system files option during the Emergency Repair Process.
After you select MS-DOS from the boot loader menu, the following error is displayed: "I/O error accessing boot sector . . . "	This message indicates that `Ntldr` can't find the `Bootsect.dos` file.	Restore this file from tape; or, perform the Emergency Repair process, selecting the Inspect boot sector option during the process.
During the boot sequence, NT displays a message indicating that it cannot find a specific file, such as `Ntoskrnl.exe` or `Ntldr`.	There are two possible causes for this problem: the specified file is missing or corrupt, or the `Boot.ini` file does not specify the correct path to system files.	To restore a missing or corrupt file (except for the `Boot.ini` file), perform the Emergency Repair process, selecting the Verify Windows NT system files option during the process. If the `Boot.ini` file is missing, perform the Emergency Repair Process, selecting the Inspect startup environment option during the process, which will create a new `Boot.ini` file. To repair a `Boot.ini` file, do one of the following: • Boot to MS-DOS and edit the `Boot.ini` file (assuming that the `Boot.ini` file is on a FAT partition) • Create a Windows NT boot diskette with the appropriate `Boot.ini`, `Ntldr`, `Ntdetect.com`, and `Bootsect.dos` files on it. Use this diskette to boot the computer to Windows NT, and then edit the `Boot.ini` file • Reinstall Windows NT (this is definitely *not* the preferred option).

continued

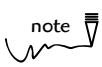
TABLE 27-1 *(continued)*

Problem	*Possible Cause*	*Recommended Solution*
Your Windows NT computer crashes during a power outage. When you reboot the computer, a blue screen is displayed during the boot sequence.	The most likely cause of this problem is a corrupt file. Power outages can easily corrupt files on the hard disk.	Perform the Emergency Repair process, selecting the Inspect boot sector and Verify Windows NT system files options during the process.
You make several configuration changes and then reboot your Windows NT computer. A blue screen is displayed during the boot sequence.	The most likely cause of this problem is the configuration changes made during the last logon session.	Reboot the computer, and select the Last Known Good Configuration during the boot sequence. If this does *not* repair the problem, perform the Emergency Repair process, selecting the Inspect Registry files option during the process.
A STOP error (blue screen) is displayed during the device driver or service initialization steps of the boot sequence.	The most probable causes of this error are a corrupt Registry entry, a corrupt device driver, or a corrupt service file.	Perform the Emergency Repair process, selecting the Inspect Registry files and Verify Windows NT system files options during the process.

Performing the Emergency Repair Process

Sometimes the only way to restore a malfunctioning Windows NT system to an operable state is to perform the Emergency Repair process. The Emergency Repair process is primarily used when you are unable to successfully boot your Windows NT computer.

The Emergency Repair process involves using the Windows NT Setup Boot Disk set, the Windows NT compact disc, and the Emergency Repair disk created during (or after) the installation process to repair a damaged or corrupt Windows NT installation.



If you didn't create an Emergency Repair disk during (or after) the Windows NT installation, an Emergency Repair disk from any other

Windows NT installation on the same hardware platform (such as Intel) can be used for *most* repair options, but *can't* be used to inspect Registry files. Also see the following caution.

caution

Never replace or repair the Registry with an Emergency Repair disk from another computer. Only repair the Registry using that specific computer's Emergency Repair Disk. Using another computer's Emergency Repair Disk can damage your computer's Windows NT installation, possibly to the point where it won't even start. This is because Registry entries are specific for an individual computer's hardware, software, policy, and user account information. No two computers have identical Registries.

The Emergency Repair process has four different repair options. During the Emergency Repair process, you are prompted to select one or more of these options. These four options are detailed in Table 27-2.

TABLE 27-2 WINDOWS NT EMERGENCY REPAIR PROCESS REPAIR OPTIONS

REPAIR OPTION	*DESCRIPTION*
Inspect Registry files	This option enables you to select any or all of the Registry files for replacement, including: • `System` (System configuration) • `Software` (Software information) • `Default` (Default user profile) • `Ntuser.dat` (New user profile) • `Security` (Security policy) • `SAM` (Security Accounts Manager user accounts database) All selected files will be replaced during the Emergency Repair process.
Inspect startup environment	Selecting this option causes Emergency Repair to verify the files in the Windows NT system partition, including: `Ntldr`, `Ntdetect.com`, `Ntbootdd.sys`, and `Boot.ini`. If any of these files are missing or corrupt, they will be replaced.

continued

TABLE 27-2 *(continued)*

Repair Option	*Description*
Verify Windows NT system files	Selecting this option causes Emergency Repair to verify the files in the Windows NT `install` folder, and to replace any missing or corrupt files from the Windows NT compact disc.
Inspect boot sector	Selecting this option causes Emergency Repair to verify that sector 0 on the active partition (also called the partition boot sector) contains the code to start `Ntldr`. If the partition boot sector is corrupt, Emergency Repair will repair it if the partition boot sector is the active partition on the first hard disk in the computer.

TO PERFORM THE EMERGENCY REPAIR PROCESS, FOLLOW THESE STEPS:

1. Start the computer using the Windows NT Setup Book Disk. Ensure that the Windows NT compact disc is in the computer's CD-ROM drive.
2. Insert Windows NT Setup Disk #2 when prompted.
3. When prompted to choose whether to repair an existing installation or to install a new copy of Windows NT, press **R** to start the Emergency Repair process.
4. The Emergency Repair menu is displayed. By default, all four options listed in Table 27-2 are selected. Deselect any options that you don't want to perform. When you're finished selecting options, select Continue from the menu.
5. Insert Windows NT Setup Disk #3 when prompted.
6. Insert the Emergency Repair Disk when prompted.
7. When the Emergency Repair process is completed, remove the floppy disk and reboot the computer to Windows NT.

If the Emergency Repair process doesn't repair your system, you may need to reinstall Windows NT.

tip **If you don't have the Windows NT Setup Boot Disk set, you can create one on an MS-DOS or Windows NT computer that has a CD-ROM drive.**

To create the Windows NT Setup Boot Disk set, place the Windows NT compact disc in the computer's CD-ROM drive. Then, from an MS-DOS command prompt, type winnt /ox and press Enter to create the disk set. Or, on a Windows NT computer, type winnt32 /ox at the command prompt and press Enter to create the disk set.

Using Event Viewer

Event Viewer is a Windows NT administrative tool that is used to view the system, security, and application logs. These logs contain success, failure, and informational messages generated by the operating system, auditing, and applications.

The most common troubleshooting application of Event Viewer is determining why a service or device driver failed during system startup. After booting the computer, Windows NT notifies the user of such a failure by displaying a Service Control Manager warning dialog box. Figure 27-1 shows a typical Service Control Manager warning dialog box.

FIGURE 27-1 **Notification of service or driver failure during startup**

When a Service Control Manager warning is displayed, you can use the Event Viewer system log to determine which service or driver failed, and to view a detailed description of the failure. This information will often help you to determine the cause of the failure and an appropriate solution.

TO ACCESS THE SYSTEM LOG IN EVENT VIEWER, FOLLOW THESE STEPS:

1. Select Start ≫ Programs ≫ Administrative Tools (Common) ≫ Event Viewer.
2. The Event Viewer dialog box appears. If the system log is not displayed, select Log ≫ System.
3. The Event Viewer System Log dialog box appears, as shown in Figure 27-2. Notice the many stop errors listed in the dialog box.

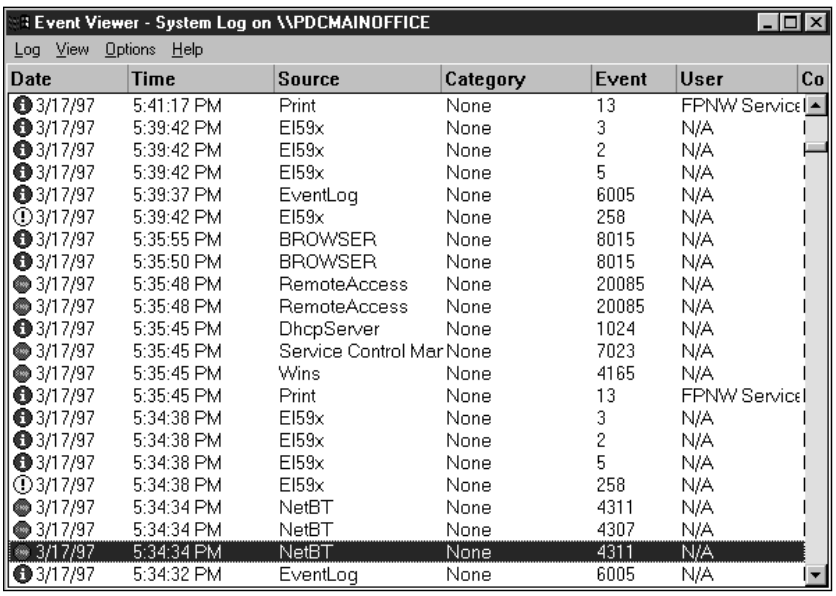


FIGURE 27-2 Viewing the system log in Event Viewer

A stop error in the system log is identified by a red stop sign preceding the event on the left-hand side of the dialog box. A *stop error* indicates that the service or driver listed in the Source column was unable to initialize correctly during system startup.

Examining stop error event details is the key to troubleshooting failed services or drivers. When multiple stop errors are listed, it's usually best to start your troubleshooting by examining the *oldest* stop error in the list first. The oldest stop error is the *first* stop error that occurred during the boot process—it is also the

last stop error on the system log list. This stop error is probably the cause of all the later stop errors listed.

To view stop error event detail, double-click the stop error in the system log in Event Viewer. When you double-click the stop error, the Event Detail dialog box is displayed, as shown in Figure 27-3. Notice the description of the stop error in the Description text box.

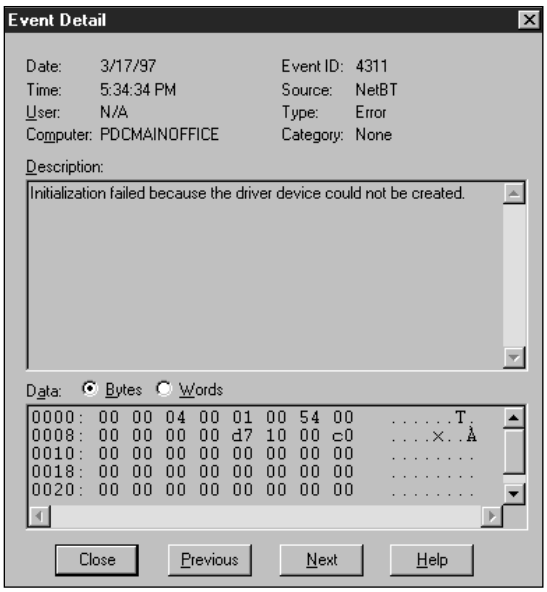


FIGURE 27-3 **Viewing stop error event detail**

The stop error detailed in Figure 27-3 indicates that initialization of the NetBT service failed because the driver device could not be created.

Sometimes the event detail provides specific information that can be used to correct the problem. Other times, further investigation using a resource such as *TechNet* may be necessary. (When using *TechNet*, I recommend searching by the complete text listed in the Event Detail Description box.)

In this case, further research determined that the NetBT device driver was corrupt, and needed to be replaced. To solve the problem, I restored the device driver from tape. Incidentally, fixing the NetBT service stop error repaired all of the other stop errors in the list.

Remember, when using Event Viewer for troubleshooting, *always* view the Event Detail for the *last* stop error in the list (the event that happened *first* chronologically during the boot process) first. Resolving this error will often take care of most or all of the other stop errors listed.

Using Windows NT Diagnostics

Windows NT Diagnostics is a Windows NT administrative tool that enables you to view detailed system configuration information and statistics. This tool can help you troubleshoot system configuration problems. It is also very useful for determining service and device driver dependencies. Windows NT Diagnostics does not actually diagnose anything—it simply displays your current system configuration information.

To access Windows NT Diagnostics, at the desktop select Start ➪ Programs ➪ Administrative Tools (Common) ➪ Windows NT Diagnostics.

The Windows NT Diagnostics dialog box appears, as shown in Figure 27-4. Notice the nine different tabs in this dialog box: Version, System, Display, Drives, Memory, Services, Resources, Environment, and Network.

The various tabs in Windows NT Diagnostics contain different options and are used for different purposes:

- **Version:** The Version tab, shown in Figure 27-4, displays this Windows NT installation's version, build number, and service pack number. It also displays the serial number and registered owner. Clicking the Print command button on any Windows NT Diagnostics tab will print details contained on *all* of the tabs in Windows NT Diagnostics. This list can be quite extensive.
- **System:** The System tab, which is shown in Figure 27-5, displays the type of *Hardware Abstraction Layer* (HAL) being used; BIOS information, including BIOS date and manufacturer; and a specific processor description for each processor in the computer.

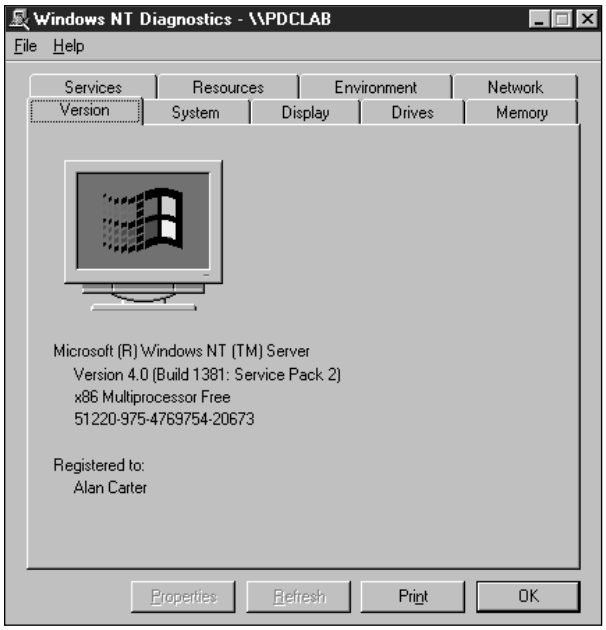


FIGURE 27-4 **The Windows NT Diagnostics initial dialog box**

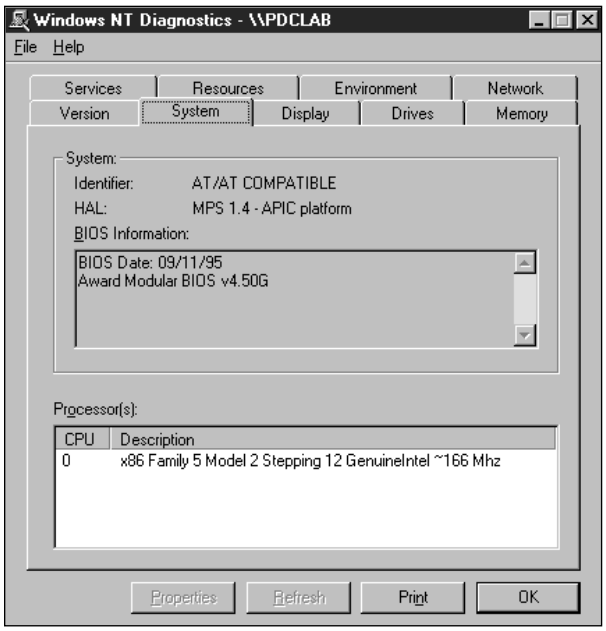


FIGURE 27-5 **The System tab in Windows NT Diagnostics**

- **Display:** The Display tab, shown in Figure 27-6, displays the display adapter configuration and the Windows NT display driver in use.

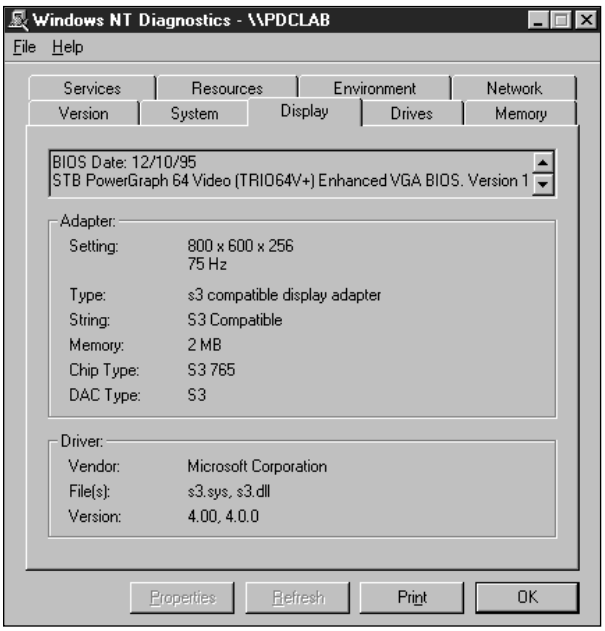


FIGURE 27-6 **The Display tab in Windows NT Diagnostics**

- **Drives:** The Drives tab, shown in Figure 27-7, displays all drives connected to this Windows NT computer, including network connected drives, if any. You can double-click any drive listed to view specific drive properties, including number of bytes free, number of bytes in use, and total number of bytes. You can also view specific file system information about the drive, such as file system type.
- **Memory:** The Memory tab, shown in Figure 27-8, displays various statistics on memory and paging file(s) in this computer. You can use these statistics to help you determine if the computer has enough memory and large enough paging files for optimum performance.
- **Services:** The Services tab, shown in Figure 27-9, displays the status of all services and device drivers installed on this Windows NT computer. Using this tab is a quick way to determine whether a particular service is running.

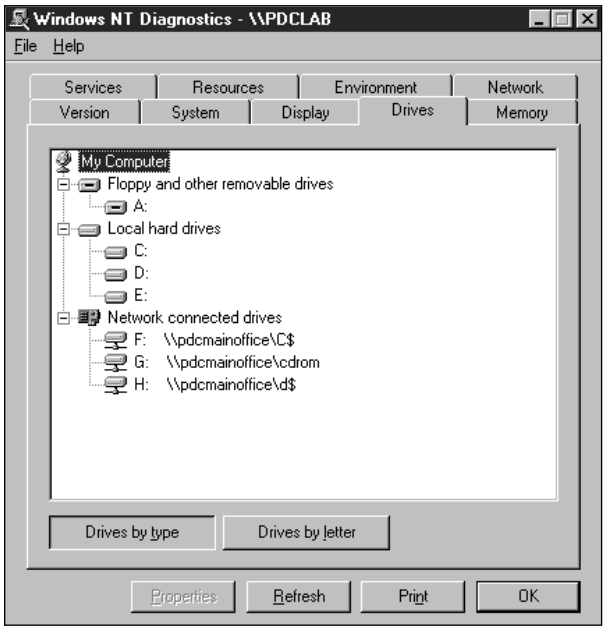


FIGURE 27-7 **The Drives tab in Windows NT Diagnostics**

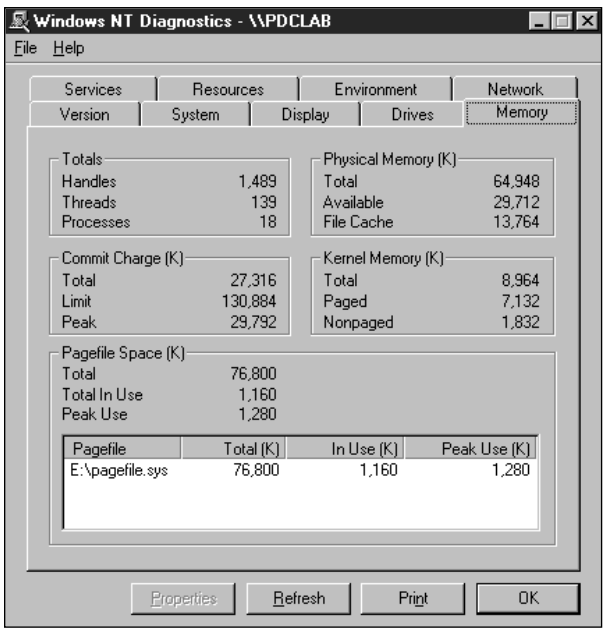


FIGURE 27-8 **The Memory tab in Windows NT Diagnostics**

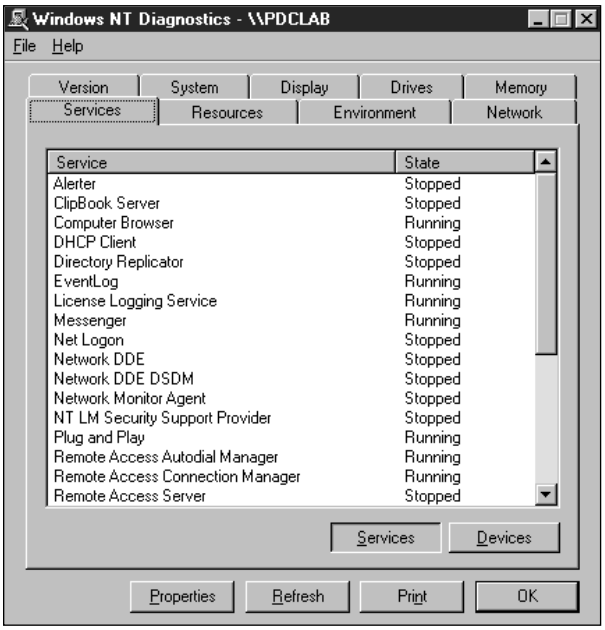


FIGURE 27-9 **The Services tab in Windows NT Diagnostics**

You can double-click any service or device driver to obtain detailed information about that service or driver.

I use this feature primarily to determine service dependencies and group dependencies for a specific service or driver — it's a lot quicker and easier than searching the Registry. *Service dependencies* show which services and drivers must be running before the service in question can start. *Group dependencies* show which groups of services or drivers must be running before the service in question can start. Once you have determined what the service and group dependencies for a particular service or driver are, you can then verify that all of these services and drivers (that are required to be running *before* a particular service or driver can start) are, in fact, running.

To determine service and group dependencies, double-click the service or driver you want to research, and then click the Dependencies tab in the Service Properties dialog box that is displayed. Figure 27-10 shows the Dependencies tab for the Computer Browser service. Notice the services that must be running before the Computer Browser service can start.

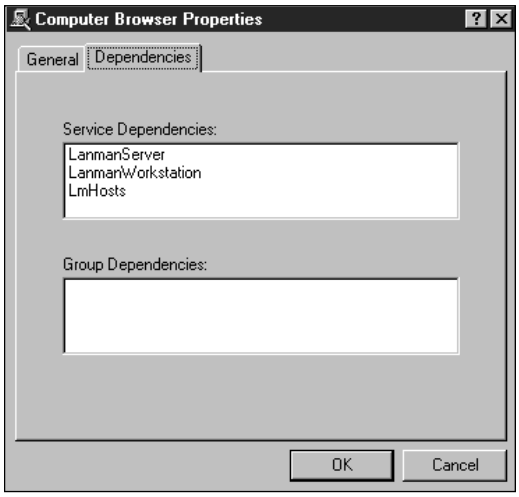


FIGURE 27-10 **Using Windows NT Diagnostics to determine service and group dependencies**

- **Resources:** The Resources tab, shown in Figure 27-11, displays the *interrupt requests* (IRQs) used by various devices in this computer. You can use this information to troubleshoot interrupt conflicts. You can also click the I/O Port, DMA, and Memory command buttons to obtain listings of all devices in this computer, by the I/O Port addresses, DMA addresses, and Memory addresses that they use. You can click the Devices command button for a listing of all devices in this computer.
- **Environment:** The Environment tab, shown in Figure 27-12, displays the system environment variables, such as the path, in use on this Windows NT computer. To obtain a list of environment variables for the user that is currently logged on to this computer, click the Local User command button.
- **Network:** The Network tab, shown in Figure 27-13, displays various network information, such as domain name and computer name. If you click the Transports or Settings command buttons, additional network configuration is displayed.

If you click the Statistics command button, numerous network utilization statistics are displayed, as shown in Figure 27-14. These statistics are not updated automatically—you must click the Refresh command button each time you want to update these statistics. These network statistics are sometimes helpful when troubleshooting network problems.

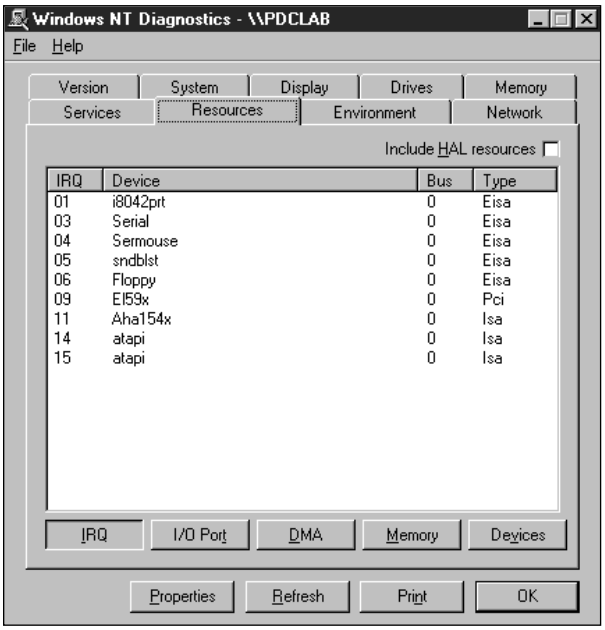


FIGURE 27-11 The Resources tab in Windows NT Diagnostics

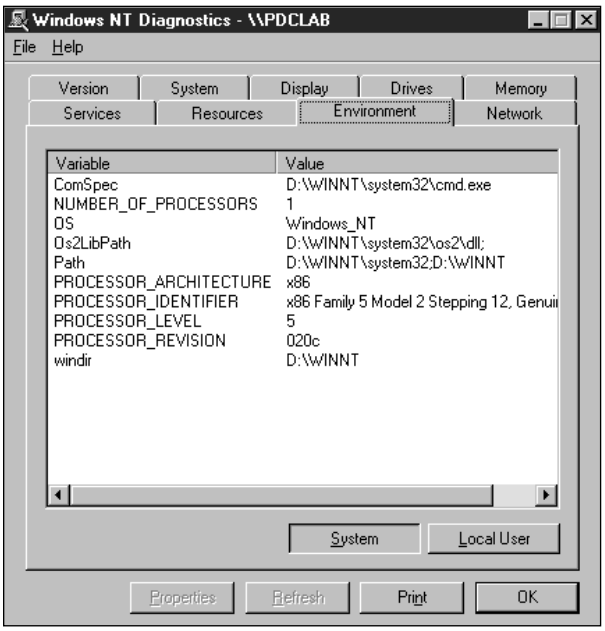


FIGURE 27-12 The Environment tab in Windows NT Diagnostics

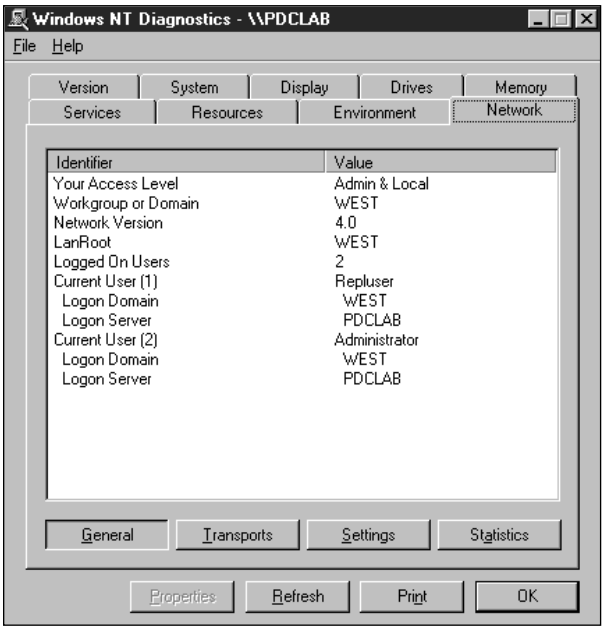


FIGURE 27-13 **The Network tab in Windows NT Diagnostics**

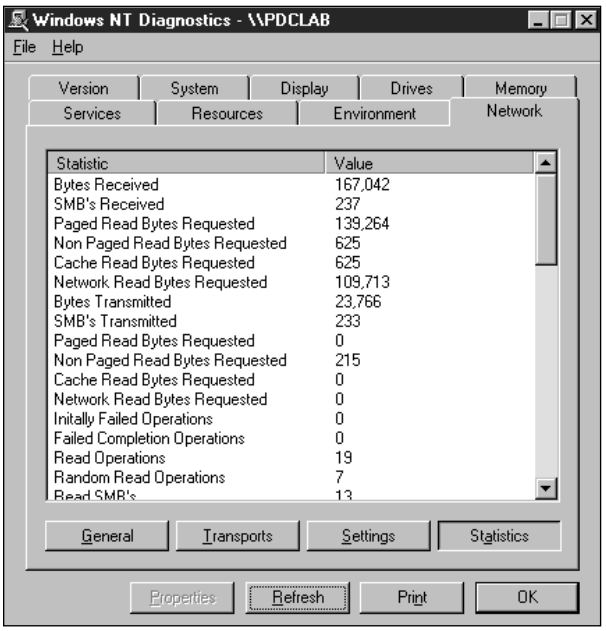


FIGURE 27-14 **Viewing network utilization statistics in Windows NT Diagnostics**

Using the Registry Editors

Registry editors are tools that enable you to search and modify the Windows NT Registry. There are two primary tools for editing the Windows NT Registry:

- Windows NT Registry Editor (`regedt32.exe`)
- Windows 95 Registry Editor (`regedit.exe`)

Additionally, you can use the Windows NT System Policy Editor (`poledit.exe`) to modify a limited number of settings in the Registry. However, you can't use System Policy Editor to search the Registry.

The Registry editors are primarily used for three types of tasks:

- To change Registry settings which can't be changed with any other user interface (such as Control Panel)
- To modify the Registry as directed by *TechNet* or by Microsoft Technical Support to resolve a particular problem or to provide a particular feature
- To troubleshoot various startup problems

The focus of this section is on using the Registry editors for troubleshooting purposes. Specifically, you'll learn how to use the Registry editors to determine service and group dependencies of various Windows NT services and device drivers.

Before explaining the specifics of how to use the Registry editors, it will be helpful for you to understand the basics of how the Windows NT Registry is structured.

Registry Structure Overview

The Windows NT Registry is a database that contains all of the information required to correctly configure an individual Windows NT computer, its user accounts, and its applications. Registries are unique to each computer—you shouldn't use the Registry from one computer on another computer. The Registry is organized in a tree structure consisting of five subtrees and their keys and value entries. Within the subtrees, keys are similar to folders in a file system, and value entries are similar to files.

Figure 27-15 shows the five subtrees within the Windows NT Registry.

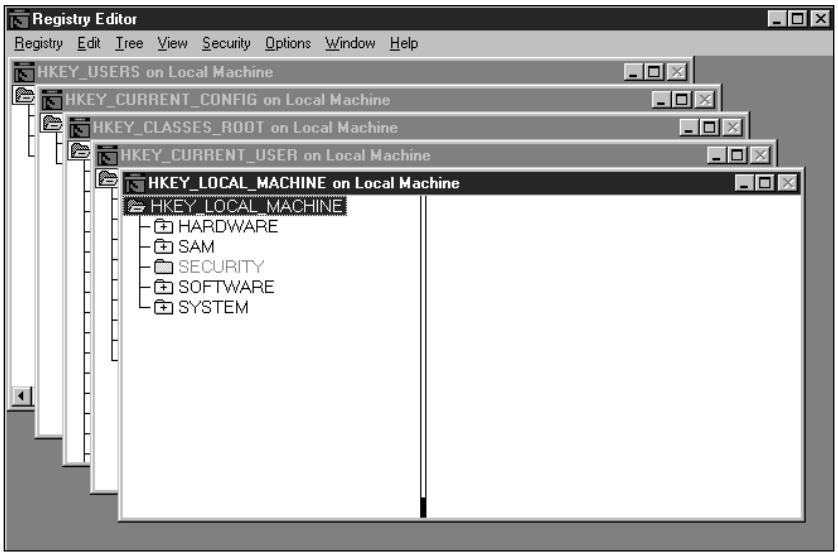


FIGURE 27-15 **The five subtrees in the Windows NT Registry hierarchy**

Each subtree in the Registry contains different types of information:

- **HKEY_LOCAL_MACHINE:** This subtree contains various configuration information specific to the local computer, including: hardware, software, device driver, and services startup configurations. Windows NT accesses this information during system startup and uses it to correctly configure the computer.

tip **When troubleshooting Windows NT, check the HKEY_LOCAL_MACHINE subtree *first*, because this subtree contains most of the service and driver configuration information for the operating system.**

- **HKEY_CURRENT_USER:** This subtree contains the entire user profile for the user that is currently logged on. This includes the user's individual desktop settings, network drive and printer connections, and so on. `HKEY_CURRENT_USER` is a replica of the keys and values stored in `HKEY_USERS\` *security identifier (SID) of currently logged on user.*
- **HKEY_CURRENT_CONFIG:** The subtree contains the hardware configuration currently being used by Windows NT. This subtree consists of a replica of the keys and values stored in `HKEY_LOCAL_MACHINE\System\CurrentControlSet\HardwareProfiles\Current`.

- **HKEY_CLASSES_ROOT:** This subtree contains all of the associations between applications and their specific filename extensions. For example, files ending in `.doc` are associated with Microsoft Word. This association is what makes it possible for you to double-click a `.doc` file and have Word start automatically and open that file. This subtree also contains all of the *object linking and embedding* (OLE) information used by various Windows applications, and consists of a replica of the keys and values stored in `HKEY_LOCAL_MACHINE\Software\Classes`.
- **HKEY_USERS:** This subtree contains the user profile for the user that is currently logged on (the current user profile), as well as the default user profile.

In the Windows NT Registry, various keys and their values are grouped together and stored in a single file. This file is called a hive. All of the Windows NT Registry hives are stored in the `<winntroot>\System32\Config` folder.

Table 27-3 shows the six hives and their respective Windows NT Registry locations.

TABLE 27-3 WINDOWS NT REGISTRY HIVES

HIVE FILE NAME	*LOCATION IN THE REGISTRY*
`SAM`	HKEY_LOCAL_MACHINE\SAM
`Security`	HKEY_LOCAL_MACHINE\Security
`Software`	HKEY_LOCAL_MACHINE\Software
`System`	HKEY_LOCAL_MACHINE\System and HKEY_CURRENT_CONFIG
`Ntuser.dat`	HKEY_CURRENT_USER
`Default`	HKEY_USERS\.DEFAULT

Now that you've got a basic understanding of the Windows NT Registry structure, you're almost ready to begin using the Registry editors. But first, it's important to back up the Registry before you use a Registry editor to modify it.

Backing Up the Registry

Always back up the Registry before you use the Registry editors to modify it—if you don't, you could end up with a system that won't boot.

There are three primary tools you can use to back up the Windows NT Registry:

- The Windows NT Backup program
- The `Regback.exe` utility included in the *Microsoft Windows NT Workstation Resource Kit*
- The `Rdisk.exe` utility

When you back up the Registry using the Windows NT Backup program, you must choose to back up at least one file on the boot partition, and you must select the check box next to the Backup Local Registry option.

When you back up the Registry using the `Rdisk.exe` utility, two backup copies are made. First, `Rdisk` makes a backup copy of the Registry and stores it in the `<winntroot>\Repair` folder. Then Rdisk prompts you to insert a floppy disk (which will become the Emergency Repair Disk), and copies the contents of the `<winntroot>\Repair` folder to the floppy disk. This process is known as *updating the Emergency Repair Disk*. Be sure to update your computer's Emergency Repair Disk every time you make a successful configuration change to your Windows NT computer.

Always run `Rdisk` using the `/s` switch, because using this switch will cause the `SAM` and `Security` hives to be backed up. If you _don't_ use the `/s` switch, these two hives won't be backed up.

It's a good idea to write the Administrator's current password on the Emergency Repair Disk when you create or update this disk. The reason for this practice is when you restore the Registry from the Emergency Repair Disk, Emergency Repair replaces whatever the Administrator's current password is with the password that was in effect when the Emergency Repair Disk was created or last updated. If the password has changed since that time, and the old password isn't written down or remembered, the Administrator won't be able to log on after the Registry is restored.

Searching the Registry

Now that you understand the structure of the Windows NT Registry and the importance of backing it up before you modify it, you can begin using the Registry editors to search and modify the Registry.

As mentioned previously, there are two primary tools you can use to edit the Windows NT Registry: the Windows NT Registry Editor (`regedt32.exe`) and the Windows 95 Registry Editor (`regedit.exe`).

I recommend you use the Windows 95 Registry Editor (`regedit.exe`) for searching the Windows NT Registry, because this editor can search the Registry by key, by value, or by the data contained in the value. As a Registry search tool, I find this editor more effective than the Windows NT Registry Editor, which can only search the Registry by key. You can manually wade your way through the various Registry folders and subfolders by using the Windows NT Registry Editor, and you can use this editor to modify any Registry value—it's just more cumbersome to use as a search tool than the Windows 95 Registry Editor.

note **While the Windows 95 Registry Editor is a better search tool, the Windows NT Registry Editor has a couple of features not included in the Windows 95 version, including the capability to connect to and edit a remote Windows NT computer's Registry, and the capability to set security on various Registry keys.**

Suppose that you recently bought a used computer that came with Windows NT installed. You want to change the Registry so that your name (not the previous owner's) is displayed as the registered owner. You are unsure where in the Registry this data is stored. However, you know the previous owner's name.

In this example, you could use the Windows 95 Registry Editor (`regedit.exe`) to search and modify the Registry.

To access the Windows 95 Registry Editor, select Start ➪ Run. Type **regedit** in the Open drop-down list box in the Run dialog box, as shown in Figure 27-16, and click OK.

The Registry Editor dialog box appears, as shown in Figure 27-17. Notice the various subtrees displayed in this dialog box.

note **Notice the HKEY_DYN_DATA subtree in the Registry Editor dialog box. This subtree only exists on Windows 95 computers. So, while this subtree is shown, it can't be opened when editing a Windows NT Registry.**

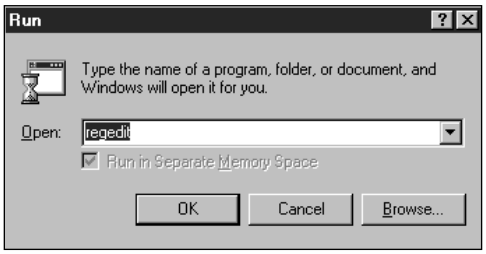


FIGURE 27-16 Starting the Windows 95 Registry Editor

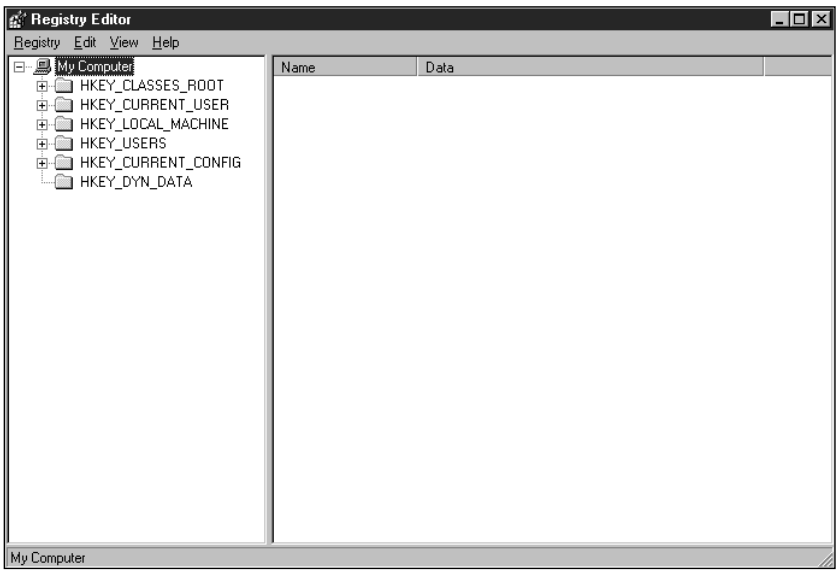


FIGURE 27-17 The Windows 95 Registry Editor dialog box

Now that the Registry Editor is started, you can use it to search the Registry for the previous owner's name.

note

The following example shows you how to search the Windows NT Registry for values that contain the previous owner's name. *However, you can use these same steps to search the Registry for any key, value, or data.*

TO SEARCH THE WINDOWS NT REGISTRY, FOLLOW THESE STEPS:

1. Select Edit ➪ Find in the Registry Editor dialog box.
2. The Find dialog box appears, as shown in Figure 27-18. Notice that three check boxes give you the option of searching by keys, values, and/or data. (You can select any or all of these options.) Type in the previous owner's name in the "Find what" text box, and click the Find Next command button.

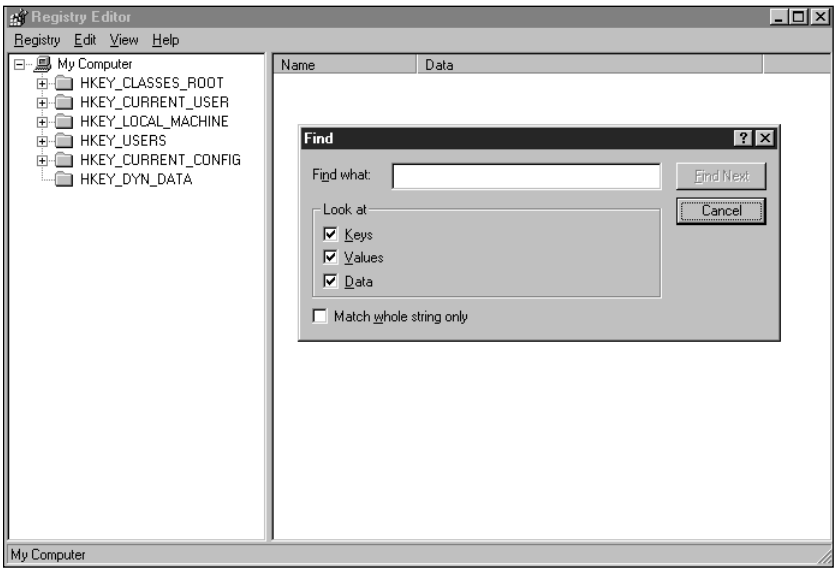


FIGURE 27-18 **Configuring the search parameters**

3. Registry Editor searches the Registry. Registry Editor displays the first instance of the previous owner's name, as shown in Figure 27-19. Notice that the complete path to the key that contains this value is shown across the bottom of the Registry Editor dialog box.

   If you want to edit the displayed value, double-click the value and edit the value's data in the Edit String dialog box that appears. Figure 27-20 shows the Edit String dialog box. Click OK when you're finished.
4. The Registry Editor dialog box reappears. To search for additional instances of the previous owner's name, select Edit ➪ Find Next. Registry Editor searches the Registry again and displays the next instance it finds of the previous owner's name.

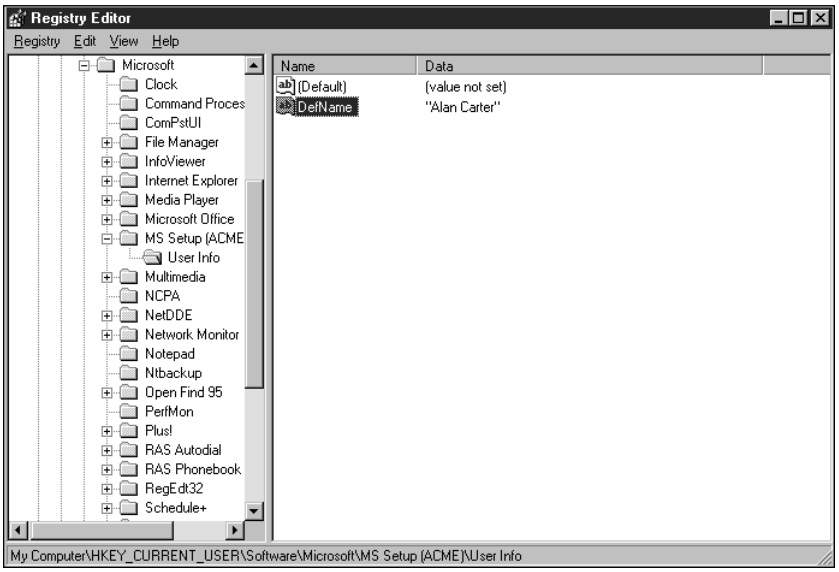


FIGURE 27-19 **Registry Editor displays search results**

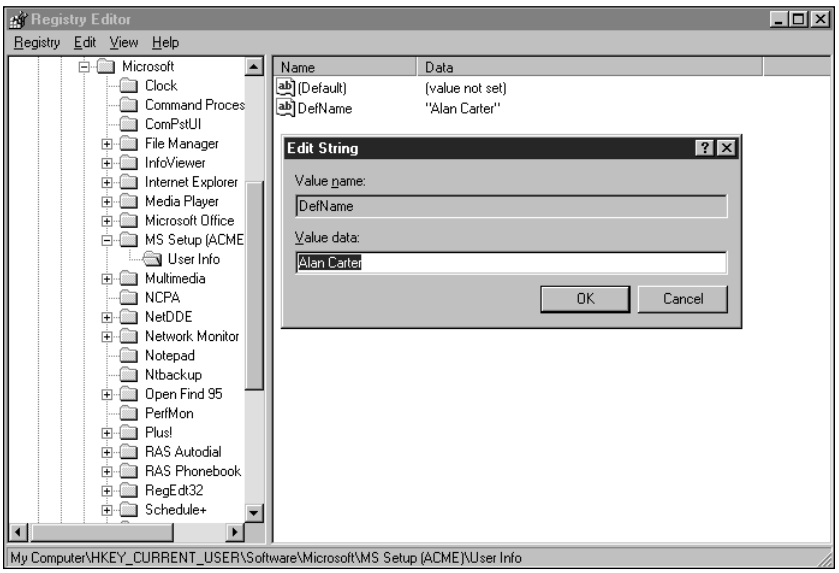


FIGURE 27-20 **Editing a value in Registry Editor**

5. Repeat Steps 3 and 4 as needed to replace all instances of the previous owner's name.
6. Exit Registry Editor when your search is completed.

Another common type of search that is performed in Registry Editor is a search for a specific service or driver, with the intent of determining the service and group dependencies of that service or driver. The next section explains how to perform such a search, and how to determine the dependencies of the service or driver.

Finding service and group dependencies

As mentioned previously, *service dependencies* show which services and drivers must be running before a particular service (or driver) can start. *Group dependencies* show which groups of services or drivers must be running before the service (or driver) in question can start. For troubleshooting purposes, once you have determined what the service and group dependencies for a particular service (or driver) are, you can then verify that all of these services and drivers (that are required to be running *before* a particular service or driver can start) are, in fact, running.

The easiest way to determine a particular service's or driver's service and group dependencies is using the Services tab in Windows NT Diagnostics, as described earlier in this chapter.

That said, you can search the Windows NT Registry to locate a particular service or driver for the purpose of determining that service's or driver's service and group dependencies.

Although you can use either Registry editor to find dependencies, only the Windows NT Registry Editor (`regedt32.exe`) presents this information in a usable format. (The Windows 95 Registry Editor presents service and group dependencies in hexadecimal format.)

If you don't know the name of the Registry key that is used to store a particular service's or driver's information, you can use the Windows 95 Registry Editor to find the key in the Registry, and then use the Windows NT Registry Editor to view the data. For example, you probably wouldn't think to look for Registry entries for the WINS Client (TCP/IP) service in a key named NetBT, but that's exactly where they are. If you didn't know this up front, you'd have to use the Windows 95 Registry Editor to determine the name of the key in which this service's entries are stored before using the Windows NT Registry Editor to view the specific data.

All service and driver Registry entries are stored in subkeys of `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services`.

Suppose you want to use a Registry editor to determine service and group dependencies of the Messenger service. (You want to do this because Event Viewer indicates that the Messenger service failed to start because a dependency service of the Messenger service was not running.)

TO USE THE WINDOWS NT REGISTRY EDITOR TO DETERMINE SERVICE AND GROUP DEPENDENCIES, FOLLOW THESE STEPS:

1. Start the Windows NT Registry Editor by selecting Start ➪ Run from the desktop, and by then typing **regedt32** in the Open drop-down list box in the Run dialog box. Then click OK.
2. If the HKEY_LOCAL_MACHINE window is not displayed, select Window ➪ HKEY_LOCAL_MACHINE on Local Machine.
3. The HKEY_LOCAL_MACHINE window is displayed. Double-click the `SYSTEM` folder. Double-click the `CurrentControlSet` folder. Double-click the `Services` folder.
4. Highlight the service or driver for which you want to determine service and group dependencies. In the example, this is the Messenger service. Various Registry entries for the highlighted service or driver are displayed on the right-hand side of the window, as shown in Figure 27-21. Notice the DependOnGroup and DependOnService entries.

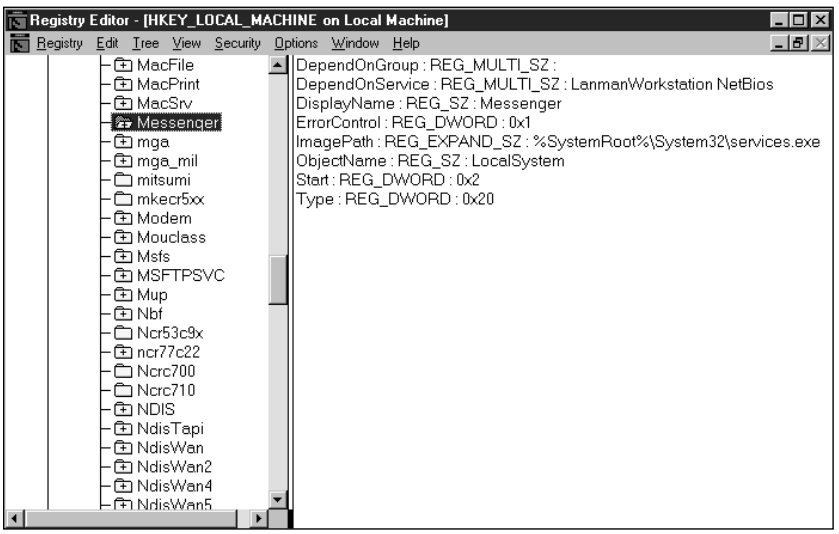


FIGURE 27-21 **Viewing the Messenger service's Registry entries**

You can ignore the REG_MULTI_SZ: portion of the DependOnGroup and DependOnService entries—REG_MULTI_SZ just identifies the type of data that will be placed in the Registry, in this case, multiple string values.

In this example, notice that the Messenger service's DependOnGroup entry does not contain any data (other than the ignored REG_MULTI_SZ). This means this service has no group dependencies.

Also notice that the Messenger's service DependOnService entry lists the LanmanWorkstation and NetBios services as its service dependencies. This means the Messenger service will not start if the LanmanWorkstation (Workstation) and the NetBios services are not running.

5. When you've finished determining a service's dependencies, exit Registry Editor.

Diagnosing and Interpreting Blue Screens

Windows NT displays a blue screen when it encounters a STOP error from which it cannot recover. Facing a blue screen is a daunting task for any network administrator. However, it's not as scary if you understand the basics of what is displayed when this happens.

It's also beneficial for you to understand blue screen contents when you contact Microsoft Technical Support personnel. If you have a basic idea what's going on, it will be easier for you to communicate with Technical Support, and may result in faster problem resolution.

If you encounter a blue screen, I recommend that you write down the blue screen's contents exactly as they are displayed on the screen. The blue screen contains information that is absolutely required by Microsoft Technical Support before they can help you troubleshoot the problem.

Most blue screens are caused by corrupt drivers or by drivers developed for a previous version of Windows NT. Most of the blue screens I have personally experi-

enced have been the result of installing third-party drivers intended for Windows NT 3.51 on a Windows NT 4.0 computer.

Listing 27-1 shows a blue screen that I generated on my Windows NT Server computer. (In case you're wondering, I generated this blue screen by installing a HAL file that was intended for use on a computer that uses a different bus architecture than mine.) Blue screens normally appear as white lettering on a blue background, thus the term "blue screen." For ease in reading, I've reproduced this blue screen with black lettering on a white background.

There are three primary sections in this displayed blue screen : the STOP error and description, a list of loaded drivers, and a stack dump (including the operating system's build number).

- **STOP error and description:** The first line at the top of the screen displays the STOP error and several hexadecimal values. The first hexadecimal value (in this case, `0x00000079`) indicates the error code for the STOP error. (The error code is sometimes referred to as a *BugCheck code*.) To determine what this error code means, you'll need a resource, such as the *Microsoft Windows NT Device Developer's Kit*. In this example, error code 79 indicates a mismatched HAL. The error code is probably the first piece of information that Microsoft Technical Support will want from you.
- **List of loaded drivers:** The second main section of the screen, which begins with the headers `Dll`, `Base`, `DateStmp`, and `Name`, contains a list of drivers that have been loaded into memory.
- **Build number and stack dump:** The third main section of the screen begins with the headers `Address`, `dword dump`, `Build [1381]`, and `Name`. This section contains the build number of the operating system (in this case, 1381). It also contains the contents of the operating system's stack. A stack is a temporary storage area used by the operating system.

Depending on your Windows NT configuration, additional information may be displayed on a blue screen. Additional lines might include information as to whether a serial port is currently being used for remote debugging purposes, and information might be displayed regarding the status of creation of the memory dump file (`memory.dmp`).

LISTING 27-1 **Sample blue screen**

```
*** STOP: 0x00000079 (0x00000003,0x00000000,0x00000002,0x00000000)

CPUID:GenuineIntel  5.2.c  irql:1   SYSVER   0xf0000565

Dll Base DateStmp - Name                    Dll Base DateStmp - Name
80100000 32add131 - ntoskrnl.exe           80010000 31ee6c55 - hal.dll
80001000 32b1cf7b - atapi.sys               80007000 328ce233 - SCSIPORT.SYS
8001b000 31f05449 - aha154x.sys            801d5000 3290d07e - Disk.sys
801d9000 32a88067 - CLASS2.SYS             801dd000 32a89744 - Ntfs.sys

Address  dword dump   Build [1381]                               - Name
80147d8c 80147fb3 80147fb3 8014b500 801c1aa4 00000000 80087000 - ntoskrnl.exe
80147d90 8014b500 8014b500 801c1aa4 00000000 80087000 00000000 - ntoskrnl.exe
80147d94 801c1aa4 801c1aa4 00000000 80087000 00000000 80144974 - ntoskrnl.exe
80147da4 80144974 80144974 80144f20 00000003 00003f9d 00000001 - ntoskrnl.exe
80147da8 80144f20 80144f20 00000003 00003f9d 00000001 0000009e - ntoskrnl.exe
80147ec0 80144d20 80144d20 80144f20 80145010 00000000 00000000 - ntoskrnl.exe
80147ec4 80144f20 80144f20 80145010 00000000 00000000 00000000 - ntoskrnl.exe
80147ec8 80145010 80145010 00000000 00000000 00000000 00000000 - ntoskrnl.exe
80147f7c 80147fb5 80147fb5 00000001 801c750e 00000001 80147fe4 - ntoskrnl.exe
80147f84 801c750e 801c750e 00000001 80147fe4 80147fe4 80147fe4 - ntoskrnl.exe
80147f8c 80147fe4 80147fe4 80147fe4 80147fe4 80147fe8 00010101 - ntoskrnl.exe
80147f90 80147fe4 80147fe4 80147fe4 80147fe8 00010101 01000101 - ntoskrnl.exe
80147f94 80147fe4 80147fe4 80147fe8 00010101 01000101 01010101 - ntoskrnl.exe
80147f98 80147fe8 80147fe8 00010101 01000101 01010101 01010101 - ntoskrnl.exe
80147fc0 80118efd 80118efd 00000000 ffdff120 0000020c 8014813c - ntoskrnl.exe
80147fd0 8014813c 8014813c 801c7193 80144f20 80148104 00000000 - ntoskrnl.exe
80147fd4 801c7193 801c7193 80144f20 80148104 00000000 80147dac - ntoskrnl.exe
80147fd8 80144f20 80144f20 80148104 00000000 80147dac 8014813c - ntoskrnl.exe
80147fdc 80148104 80148104 00000000 80147dac 8014813c 801c721a - ntoskrnl.exe
80147fe4 80147dac 80147dac 8014813c 801c721a 00000000 80087000 - ntoskrnl.exe
80147fe8 8014813c 8014813c 801c721a 00000000 80087000 80036c00 - ntoskrnl.exe
81047fec 801c721a 801c721a 00000000 80087000 80036c00 801c6678 - ntoskrnl.exe
80147ffc 801c6678 801c6678 80144f20 00000000 00000000 00000000 - ntoskrnl.exe
80148000 80144f20 80144f20 00000000 00000000 00000000 00000000 - ntoskrnl.exe
80148080 80140764 80140764 00000000 00000000 00000000 00000000 - ntoskrnl.exe
80148124 80147ff8 80147ff8 00000000 ffffffff 80139074 80142a80 - ntoskrnl.exe
80148130 80139074 80139074 80142a80 00000000 00000000 801c5e50 - ntoskrnl.exe
80148134 80142a80 80142a80 00000000 00000000 801c5e50 80144d20 - ntoskrnl.exe
80148140 801c5e50 801c5e50 80144d20 80144f20 80148160 ffdff120 - ntoskrnl.exe
80148144 80144d20 80144d20 80144f20 80148160 ffdff120 00000000 - ntoskrnl.exe
80148148 80144f20 80144f20 80148160 ffdff120 00000000 80087000 - ntoskrnl.exe
8014814c 80148160 80148160 ffdff120 00000000 80087000 0000000e - ntoskrnl.exe
```

Configuring a Memory Dump

Sometimes Microsoft Technical Support won't be able to help you quickly resolve a blue screen. Microsoft may need to analyze the contents of the memory dump file created when the blue screen occurred.

To ensure that Windows NT will create a memory dump file when a STOP error occurs, you can use the System application in the Control Panel to make sure Windows NT is appropriately configured.

TO CONFIGURE WINDOWS NT TO CREATE A MEMORY DUMP FILE (MEMORY.DMP), FOLLOW THESE STEPS:

1. Select Start ➪ Settings ➪ Control Panel.
2. In the Control Panel dialog box, double-click the System icon.
3. The System Properties dialog box appears. Click the Startup/Shutdown tab.
4. The Startup/Shutdown tab appears, as shown in Figure 27-22. Notice the Recovery section in this dialog box.

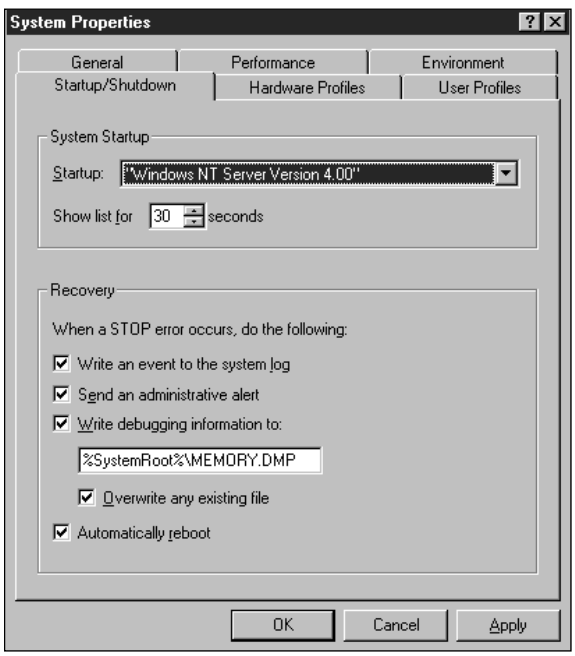


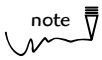
FIGURE 27-22 **Configuring Windows NT recovery options**

Ensure that the check boxes next to "Write debugging Information to" and "Overwrite any existing file" are selected.

Ensure that the text box in the Recovery section contains the following: `%SystemRoot%\MEMORY.DMP`

Click OK.

5. Exit Control Panel. You should shut down and restart your computer for these changes to become effective.



To create a `memory.dmp` file, Windows NT requires a paging file on the boot partition of the system disk that is at least as large as the amount of RAM in the computer.

There are two utilities that you can use to examine the `memory.dmp` file: `Dumpchk.exe`, and `Dumpexam.exe`. Both utilities can be found on the Windows NT compact disc in the `Support\Debug\i386` folder. Normally these utilities are used as directed by Microsoft Technical Support.

The `Dumpchk` utility is used to check the `memory.dmp` file to ensure that it can be correctly read by a kernel debugger. Microsoft recommends that you use the `Dumpchk` utility before you send the `memory.dmp` file to Microsoft Technical Support for debugging. If you have to send the `memory.dmp` file to Microsoft via the Internet or a modem, use a compression utility (such as PKZIP or WinZip) to compress the file before you send it.

The `Dumpexam` utility is used to analyze the `memory.dmp` file and extract specific types of information from this file. The `Dumpexam` utility then places this information in a text file, usually `memory.txt`. The `memory.txt` file is normally small enough to be e-mailed directly to Microsoft Technical Support, or you can print it out and fax it.

Configuring Dr. Watson for Windows NT

Dr. Watson for Windows NT is a tool that is used to debug application errors. Dr. Watson detects application errors as they occur, analyzes the error, and logs error

information to a log file.

Additionally, Dr. Watson for Windows NT can be configured to create an application dump file that can be analyzed by a more sophisticated application debugger. You might use this application dump file feature at the request of your application developer if you're having application problems.

Windows NT automatically starts Dr. Watson when an application error occurs. By default, Dr. Watson is configured to create an application dump file. You may want to ensure that Dr. Watson is configured correctly, or change Dr. Watson's configuration. Before you can configure Dr. Watson for Windows NT, you must start Dr. Watson manually from the Run dialog box.

TO MANUALLY START DR. WATSON FOR WINDOWS NT AND TO ENSURE THAT DR. WATSON IS CONFIGURED CORRECTLY, FOLLOW THESE STEPS:

1. From the Windows NT desktop, select Start ➪ Run.
2. The Run dialog box appears. In the Open drop-down list box, type **drwtsn32** and click OK.
3. The Dr. Watson for Windows NT dialog box appears, as shown in Figure 27-23. Notice that, by default, Dr. Watson is configured to create a log file and to dump application memory to a file named `user.dmp` when an application fails.

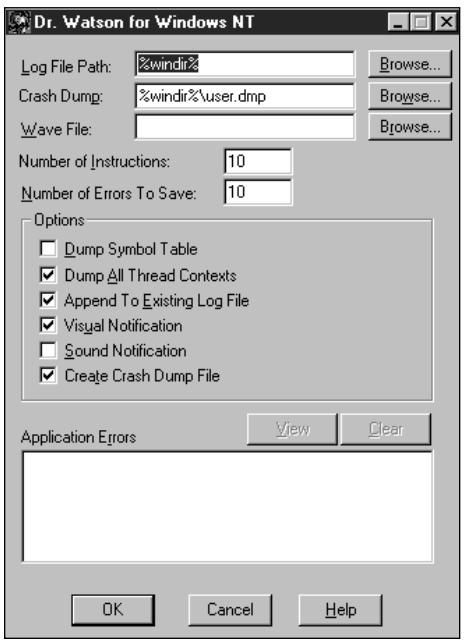


FIGURE 27-23 **Configuring Dr. Watson for Windows NT**

Ensure that the Crash Dump text box reads as follows:
`%windir%\user.dmp`.

Ensure that the check boxes next to: Dump All Thread Contexts, Append To Existing Log File, Visual Notification, and Create Crash Dump File are selected.

Click OK. Windows NT closes Dr. Watson for Windows NT automatically.

Configuring a Computer for Remote Debugging

Occasionally Microsoft Technical Support may not be able to resolve a problem by analyzing a blue screen or by analyzing a memory dump file. In this situation, Microsoft may need to remotely connect to the computer experiencing the problem and actively debug the computer. The tool that Microsoft Technical Support uses to remotely debug the computer is the *Kernel Debugger*.

Three computers are involved in the debugging process: the computer being debugged (the *target computer*), an additional Windows NT computer at your site (the *host computer*), and a computer at Microsoft Technical Support.

Both the target and host computers need to be running the same version of Windows NT, and you need to connect the two computers using a null-modem cable.

Normally it will be your job to configure the target and host computers at your site for the debugging session. Ask Microsoft Technical Support if they want you to configure your computers for remote debugging before proceeding with the steps listed below.

Configuring the Target Computer

This section explains how to configure the target computer at your site for remote debugging.

TO CONFIGURE THE TARGET COMPUTER FOR REMOTE DEBUGGING, FOLLOW THESE STEPS:

1. Connect one end of the null-modem cable to the COM2 port on the target computer. (If you only have one COM port, or if you have a serial mouse connected to COM2, connect the null-modem cable to COM1.)
2. Edit the `Boot.ini` file on the target computer by adding `/DEBUG` to the end of the ARC pathname that you use to boot the computer.

   The following is a `Boot.ini` file that has been correctly configured for remote debugging:

   ```
   [boot loader]
   timeout=30
   default=multi(0)disk(0)rdisk(1)partition(1)\WINNT
   [operating systems]
   multi(0)disk(0)rdisk(1)partition(1)\WINNT="Windows NT
        Server Version 4.00" /DEBUG
   multi(0)disk(0)rdisk(1)partition(1)\WINNT="Windows NT
        Server Version 4.00 [VGA mode]" /basevideo /sos
   C:\="Microsoft Windows"
   ```

3. Shut down and reboot the target computer to Windows NT.

Configuring the Host Computer

This section explains how to configure the host computer at your site for a remote debugging session.

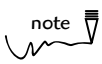
TO CONFIGURE THE HOST COMPUTER, FOLLOW THESE STEPS:

1. Connect the other end of the null-modem cable to any available COM port on the host computer.
2. Place the Windows NT compact disc in the host computer's CD-ROM drive. Select Start ≥ Programs ≥ Command Prompt.

3. At the Command Prompt, type in the drive letter of the CD-ROM drive followed by a colon (for example, D:) and press Enter.

   Type **\support\debug\expndsym.cmd <*your_CD-ROM_drive_letter*:> <*full_path_to_your_Windows_NT_installation*>** and press Enter. For example, on a Windows NT computer that has a CD-ROM on drive D:, and has Windows NT installed in `c:\winnt`, the command would be as follows: `\support\debug\expndsym.cmd d: c:\winnt`. (Don't type the period at the end.)

   This command line installs the Windows NT debugger and all of the Windows NT symbol files required by the debugger.



If you've installed any service packs on your Windows NT host computer, you must also install all of the symbol files from the service pack(s) at this point.

4. Install and configure RAS on the host computer if it is not already installed and configured. Don't configure RAS to use the COM port to which the null-modem cable is connected. You must configure RAS with at least one dial in port so that Microsoft Technical Support can remotely access this computer. (Installing and configuring RAS is covered in Chapter 19.)

   Note: If you don't want to install RAS on the host computer, RAS can be installed on another Windows NT computer on the same network as the host computer.

5. Just before Microsoft Technical Support connects to the host computer via a RAS connection, select Start ➪ Programs ➪ Command Prompt, and type the following commands at the Command Prompt (Press Enter after each command):

   set nt_debug_port=com1 (or the COM port on the host computer that the null-modem cable is connected to, if not COM1)

   set nt_debug_baud_rate=19200

   set nt_symbol_path=c:\winnt\symbols (or the path to your Windows NT installation, if not `c:\winnt`)

   set nt_log_file_open=c:\debug.log

   remote /s "i386kd -v" debug

   At this point, all of the environment variables required for remote debugging are configured on the host computer, and the `Remote.exe` utility and the debugger are running.

6. After Microsoft Technical Support connects to the host computer via RAS, the Microsoft technician will type remote /c *host_computer_name* debug at a command prompt on a computer at the Microsoft site to connect to the debugger on the host computer.

Key Point Summary

exam preparation pointer

Many of the topics in this chapter are very dry. You will hopefully not need to use this information very often. However, you should study this entire chapter carefully before you take any of the Windows NT 4.0 Certified Professional exams.

Chapter 27 covered advanced troubleshooting topics, including solutions to common boot sequence problems; how and when to use the Event Viewer and Windows NT diagnostics; how to search and modify the Registry; how to interpret blue screens, and how to set up and use memory dumps, Dr. Watson, and remote debugging.

- The boot sequence refers to the process of starting Windows NT, including initializing all of its services and completing the logon process. To successfully troubleshoot problems that can occur during this process, you need an understanding of the steps that occur during the boot sequence. The steps in the Windows NT boot sequence (for the Intel platform only) are:
  - Power On Self Test (POST)
  - Initial Startup
  - Selecting an operating system
  - Detecting hardware
  - Selecting hardware profile (or Last Known Good Configuration) and loading the kernel
  - Kernel initialization
  - Initializing device drivers
  - Initializing services
  - Logon process

- Table 27-1, Troubleshooting the Windows NT Boot Sequence, lists many common problems that can occur during the boot sequence, along with their possible causes and recommended solutions. Refer to this table now and review it. Review it again just before taking any of the three Windows NT exams. Note that the Emergency Repair process is part of many solutions to boot sequence problems.
- The *Emergency Repair process* involves using the Windows NT Setup Boot Disk set, the Windows NT compact disc, and the Emergency Repair disk created during (or after) the installation process to repair a damaged or corrupt Windows NT installation. There are four different repair options in the Emergency Repair Process. You can select one or more of these options: Inspect Registry files, Inspect startup environment, Verify Windows NT system files, and Inspect boot sector.
- *Event Viewer* is a Windows NT administrative tool used to view the system, security, and application logs. When a Service Control Manager warning message is displayed during bootup, indicating that a service or driver failed to start, you can use the Event Viewer system log to determine which service or driver failed, and to view a detailed description of the failure. When examining stop errors in the system log, it's usually most efficient to examine the event that took place first—the last event in the list—first. Solving the oldest error often solves all other errors listed.
- *Windows NT Diagnostics* is a Windows NT administrative tool that enables you to view detailed system configuration information and statistics. This tool can help you troubleshoot system configuration problems, and also help you determine service and device driver dependencies. The Services tab in Windows NT Diagnostics is particularly useful for determining service and group dependencies for a specific service or driver.
- *Registry editors* are tools that enable you to search and modify the Windows NT Registry. There are two primary tools for editing the Windows NT Registry: the Windows NT Registry Editor (`regedt32.exe`) and the Windows 95 Registry Editor (`regedit.exe`). Before getting into the specifics of how to use the Registry editors, it's helpful to have a basic understanding of how the Windows NT Registry is structured.

- The Windows NT Registry is a database that contains all of the information required to correctly configure an individual Windows NT computer, its user accounts, and applications. The Registry is organized in a tree structure consisting of five subtrees and their keys and value entries. The five subtrees of the Registry are: HKEY_LOCAL_MACHINE, HKEY_CURRENT_USER, HKEY_CURRENT_CONFIG, HKEY_CLASSES_ROOT, and HKEY_USERS. The HKEY_LOCAL_MACHINE subtree is the most helpful subtree in terms of troubleshooting because it contains most of the service and driver configuration information for the operating system.
- *Always* back up the Registry before you use the Registry editors to modify it. You can use the Windows NT Backup program, the `Regback.exe` utility, or the `Rdisk.exe` utility to back up the Registry on your Windows NT computer. If you use `Rdisk`, always run this utility using the `/s` switch, so that the `SAM` and `Security` hives will be backed up.
- Use the Windows 95 Registry Editor to search the Registry, because this editor can search the Registry by key, by value, or by the data contained in the value. The Windows NT Registry, on the other hand, can only search the Registry by key. To access the Windows 95 Registry Editor, select Start ➪ Run from the desktop. Then type **regedit** in the Open drop-down list box in the Run dialog box, and click OK.

- *Service dependencies* show which services and drivers must be running before a particular service (or driver) can start. *Group dependencies* show which groups of services or drivers must be running before the service (or driver) in question can start. For troubleshooting purposes, once you have determined what the service and group dependencies for a particular service (or driver) are, you can then verify that all of these services and drivers (that are required to be running *before* a particular service or driver can start) are, in fact, running.
- The easiest way to determine a particular service's or driver's service and group dependencies is to use Windows NT Diagnostics. However, you can also determine dependencies by using the Windows NT Registry Editor (`regedt32.exe`). To access the Windows NT Registry Editor, select Start ➪ Run from the desktop. Then type **regedt32** in the Open drop-down list box in the Run dialog box, and click OK.

- All service and driver Registry entries are stored in subkeys of `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services`
- Windows NT displays a *blue screen* when it encounters a STOP error from which it can't recover. Most blue screens are caused by corrupt drivers or by drivers developed for a previous version of Windows NT. There are three primary sections in a blue screen: the STOP error (including error code or BugCheck code) and description, a list of loaded drivers, and a stack dump (including the operating system's build number).
- You can use the System application in Control Panel to ensure that Windows NT is correctly configured to create a *memory dump file* (`memory.dmp`) when a STOP error occurs. There are two utilities that you can use to examine the memory dump file: `Dumpchk.exe` and `Dumpexam.exe`.
- *Dr. Watson for Windows NT* is a tool used to debug application errors. Windows NT automatically starts Dr. Watson when an application error occurs. By default, Dr. Watson is configured to create an application dump file.
- Occasionally, Microsoft Technical Support may need to remotely connect to a computer experiencing a problem and actively debug the computer. Three computers are involved in the debugging process: the computer being debugged (the target computer), an additional Windows NT computer at your site (the host computer), and a computer at Microsoft Technical Support. Both the target and host computers need to be running the same version of Windows NT, and you need to connect the two computers by using a null-modem cable. Normally, you will be responsible for configuring the target and host computers at your site for the debugging session.

Applying What You've Learned

Now it's time to regroup, review, and apply what you've learned in this chapter.

The review questions in the following Instant Assessment section bring to mind key facts and concepts. In addition, some of the questions give you a chance

to analyze a situation and apply your troubleshooting knowledge of Windows NT to that particular situation.

The hands-on lab exercise will reinforce what you've learned, and provide an opportunity for you to practice some of the tasks tested by the Microsoft Certified Professional exams.

Instant Assessment

1. Briefly list the nine major steps in the Windows NT boot sequence.
2. Your Windows NT computer crashes during a power outage. When you reboot the computer, a blue screen is displayed during the boot sequence. What is the most likely cause of this problem, and what should you do to resolve it?
3. You make several configuration changes and then reboot your Windows NT computer. A blue screen is displayed during the boot sequence. What is the most likely cause of this problem, and what should you do to resolve it?
4. What does the Emergency Repair process involve?
5. You receive a Service Control Manager warning message that indicates that a service or device driver failed during system startup. Which Windows NT administrative tool should you use to obtain more information about the failure?
6. When using the system log in Event Viewer for troubleshooting, for which stop error should you view the Event Detail first?
7. What are service dependencies and group dependencies?
8. Which tab in Windows NT Diagnostics is useful for determining service and group dependencies for a specific service or driver?
9. Name the two Registry editors.
10. When you are troubleshooting Windows NT, which subtree in the Registry should you normally check first?
11. What should you always do to the Registry before you modify it?
12. Which switch must you use with the `Rdisk` utility if you want the `SAM` and `Security` hives to be backed up?

13. Which of the two Registry editors is a better tool for searching the Registry, and why?
14. Which of the two Registry editors is more useful for viewing the service and group dependencies of a particular service?
15. When does Windows NT display a blue screen?
16. What are the three main sections in a blue screen?
17. Which Control Panel application can you use to ensure that Windows NT is configured to create a memory dump file (`memory.dmp`) when a STOP error occurs?
18. Which Windows NT tool is used to debug application errors?

For answers to the Instant Assessment questions see Appendix D.

Hands-on Lab Exercise

The following hands-on lab exercise provides you with a practical opportunity to apply the Windows NT troubleshooting knowledge you've gained in this chapter.

Lab 27.39 *Troubleshooting Windows NT*

Workstation
Enterprise

The purpose of this lab exercise is to give you experience in using advanced Windows NT troubleshooting techniques.

This lab consists of four parts:

Part 1: Using Windows NT Diagnostics
Part 2: Using the Registry editors
Part 3: Configuring a memory dump
Part 4: Starting and configuring Dr. Watson for Windows NT

Begin this lab by booting your computer to Windows NT Server. Log on as Administrator.

Follow these instructions carefully.

Part 1: Using Windows NT Diagnostics

In this section you use Windows NT Diagnostics to examine your Windows NT Server system configuration and to view service dependencies and group dependencies.

1. Select Start ≫ Programs ≫ Administrative Tools (Common) ≫ Windows NT Diagnostics.

2. The Windows NT Diagnostics dialog box appears. Click the System tab.
3. The System tab appears. Notice the BIOS and CPU information displayed on this tab. Click the Display tab.
4. The Display tab appears. Notice the display adapter and driver settings. Click the Drives tab.
5. The Drives tab appears. Click the + sign next to Local hard drives. Highlight drive D: (or the letter of your NTFS drive, if not D:). Click the Properties command button.
6. The Properties dialog box appears. Notice the statistics on the number of bytes free, used, and total that are presented. Click OK. Click the Memory tab.
7. The Memory tab appears. Notice the memory and pagefile statistics displayed. Click the Network tab.
8. The Network tab appears. Notice the various network information that is displayed. Click the Statistics command button. Notice the statistics that are displayed. These statistics are not updated automatically—you must click the Refresh command button to update these statistics. Click the Resources tab.
9. The Resources tab appears. Notice that you can obtain Interrupt (IRQ), I/O Port, DMA, and memory information on this tab. Click the Devices command button. Double-click Floppy in the Device list box.
10. The Floppy Properties dialog box appears. Notice the resource settings displayed. Click OK. Click the Services tab.
11. The Services tab appears. Click the Devices command button.
12. In the Device list box, scroll down and double-click Parallel.
13. The Parallel Properties dialog box appears. Click the Dependencies tab.
14. The Dependencies tab appears. Notice the Service Dependencies and Group Dependencies listed. In the space provided, write down the following, as shown on your monitor:

    Service Dependencies: _____

    Group Dependencies: _____

    Click OK.
15. The Services tab reappears. Click the Services command button.
16. Double-click the Server service.
17. The Server Properties dialog box appears. Click the Dependencies tab.

18. The Dependencies tab appears.

    In the space provided, write down the following, as shown on your monitor: Service Dependencies: _____

    Group Dependencies: _____

    Click OK.
19. The Services tab reappears. Click OK. Proceed to Part 2.

Part 2: Using the Registry editors

In this section you use the `Regedit.exe` and `Regedt32.exe` Registry editors to search the Registry, and to view service dependencies and group dependencies.

1. Select Start ➪ Run.
2. The Run dialog box appears. In the Open drop-down list box, type **regedit** and click OK. (This starts the Windows 95 Registry Editor.)
3. The Registry Editor dialog box appears. Select Edit ➪ Find.
4. The Find dialog box appears. In the Find what text box, type **WINS Client**. Ensure that the check boxes next to Keys, Values, and Data are checked. Click the Find Next command button.
5. Registry Editor searches the Registry. (This may take a few minutes.) The Registry Editor dialog box reappears. Notice that the Title value is highlighted on the right-hand side of the screen. Also notice that the Registry location of the highlighted value is displayed across the bottom of the dialog box.
6. Select Edit ➪ Find Next.
7. Registry Editor searches the Registry. The Registry Editor dialog box reappears. Notice that a different value, DeviceDesc, is highlighted. Again, notice that the Registry location of this value is displayed across the bottom of the dialog box.
8. Exit Registry Editor.
9. Select Start ➪ Run.
10. The Run dialog box appears. In the Open drop-down list box, type **regedt32** and click OK. (This starts the Windows NT Registry Editor.)
11. The Registry Editor dialog box appears. Select Window ➪ HKEY_LOCAL_MACHINE on Local Machine.
12. Maximize the Registry Editor dialog box and the HKEY_LOCAL_MACHINE on Local Machine window.
13. Double-click the `SYSTEM` folder.
14. Double-click the `CurrentControlSet` folder.

15. Double-click the `Services` folder.

16. Scroll down and highlight the `Parallel` folder. Notice the DependOnGroup and DependOnService entries on the right-hand side of the dialog box.

In the space provided, write down the entries that follow these values: (You can ignore the REG_MULTI_SZ: portion of the entries—this just identifies the type of data that will be placed in the Registry, in this case, multiple string values.)

DependOnGroup: _____

DependOnService: _____

Notice that the DependOnGroup and DependOnService values are the same as the Group Dependencies and Service Dependencies that you found using Windows NT Diagnostics in Step 14 in Part 1 of this lab.

17. On the left side of the Registry Editor dialog box, scroll up and highlight the `LanmanServer` folder. Notice the DependOnGroup and DependOnService entries on the right-hand side of the dialog box.

In the space provided, write down the entries that follow these values: (You can ignore the REG_MULTI_SZ: portion of the entries.)

DependOnGroup: _____

DependOnService: _____

Notice that the DependOnGroup and DependOnService values are the same as the Group Dependencies and Service Dependencies that you found using Windows NT Diagnostics in Step 18 in Part 1 of this lab.

Also notice the DisplayName value on the right-hand side of the dialog box. The LanmanServer service is the same as the Server service.

18. Exit Registry Editor. Proceed to Part 3.

Part 3: Configuring a memory dump

In this section you use the System application in Control Panel to ensure that Windows NT Server is correctly configured to automatically dump memory when a STOP error occurs.

Then you use the System application to configure Windows NT Workstation to automatically dump memory when a STOP error occurs.

1. Select Start ➪ Settings ➪ Control Panel.

2. The Control Panel dialog box appears. Double-click the System icon.

3. The System Properties dialog box appears. Click the Startup/Shutdown tab.

4. The Startup/Shutdown tab appears. In the Recovery section of the dialog box, ensure that all check boxes are selected. Also ensure that the text box reads as follows: `%SystemRoot%\MEMORY.DMP`. Click OK.
5. Exit Control Panel.
6. Select Start ➪ Shut Down.
7. In the Shut Down Windows dialog box, click the radio button next to "Restart the computer." Click the Yes command button.
8. Reboot your computer to Windows NT Workstation. Log on as Administrator.
9. Select Start ➪ Settings ➪ Control Panel.
10. The Control Panel dialog box appears. Double-click the System icon.
11. The System Properties dialog box appears. Click the Startup/Shutdown tab.
12. The Startup/Shutdown tab appears. In the Recovery section of the dialog box, select all of the check boxes. Also ensure that the text box reads as follows: `%SystemRoot%\MEMORY.DMP`. Click OK.
13. A System Control Panel Applet dialog box appears, indicating that the Alerter service is not running. Click OK.
14. A System Settings Change dialog box appears. Click the No command button (don't reboot your computer at this time).
15. The Control Panel dialog box reappears. Double-click the Services icon.
16. The Services dialog box appears. Highlight the Alerter service. Click the Startup command button.
17. The Service dialog box appears. In the Startup Type section, select the radio button next to Automatic. Click OK.
18. In the Services dialog box, click the Close command button.
19. Exit Control Panel. Proceed to Part 4.

Part 4: Starting and configuring Dr. Watson for Windows NT

In this section you manually start Dr. Watson for Windows NT, and verify that Dr. Watson is configured to automatically dump application memory when an application fails.

1. Select Start ➪ Run.
2. The Run dialog box appears. In the Open drop-down list box, type **drwtsn32** and click OK.

3. The Dr. Watson for Windows NT dialog box appears. Notice that, by default, Dr. Watson is configured to create a log file and to dump application memory to a file named user.dmp when an application fails.

Ensure that the Crash Dump text box reads as follows:

```
%windir%\user.dmp
```

Ensure that the check boxes next to: Dump All Thread Contexts, Append To Existing Log File, Visual Notification, and Create Crash Dump File are selected.

Click OK. Window NT closes Dr. Watson for Windows NT automatically.