Previous screen

50-30-19 Windows NT Architecture

Gilbert Held

Payoff

Windows NT is a sophisticated operating system for workstations and network servers. This article helps network managers to understand the communications capability of workstations and servers running on Windows NT, and data base administrators to determine the suitability of this platform for a structured query language (SQL) data base server.

Introduction

Windows NT is a 32-bit, preemptive multitasking operating system that includes comprehensive networking capabilities and several levels of security. Microsoft markets two version of Windows NT: one for workstations—appropriately named Windows NT Workstation—and a second for servers—Windows NT Server. This article, which describes the workings of the NT architecture, collectively references both versions as Windows NT when information is applicable to both versions of the operating system. Similarly, it references a specific version of the operating system when the information presented is specific to either Windows NT Workstation or Windows NT Server.

Architecture

Windows NT consists of nine basic modules. The relationship of those modules to one another, as well as to the hardware platform on which the operating system runs, is illustrated in Exhibit 1.

Windows NT Core Modules

Hardware Abstraction Layer

The hardware abstraction layer (HAL) is located directly above the hardware on which Windows NT operates. HAL actually represents a software module developed by hardware manufacturers that is bundled into Windows NT to allow it to operate on a specific hardware platform, such as Intel X86, DEC Alpha, or IBM PowerPC.

HAL hides the specifics of the hardware platform from the rest of the operating system and represents the lowest level of Windows NT. Thus, HAL provides true hardware platform independence for the operating system.

Using HAL, software developers can create new software without a lot of knowledge about the hardware platform. This allows software developers to provide enhanced performance capabilities, such as additional device drives. Hardware vendors can provide the interface between the operating system and the specific hardware.

Kernel

The kernel represents the core of the Windows NT operating system. All operating systems have a kernel. The key difference between the Windows NT kernel and those found in other operating systems is the tasks managed.

Previous screen

The Windows NT kernel manages thread dispatching. (A “thread” is a basic item that can be scheduled by the kernel.) The kernel is also responsible for scheduling and processor synchronization when the hardware platform has multiple processors.

To perform scheduling, the Windows NT kernel attempts to dispatch threads for execution in a way that promotes the most efficient use of the processors in the hardware platform. The actual dispatching of threads is based on their priority, with Windows NT supporting 32 priority levels to maximize processor use.

The kernel always resides in real memory within the hardware platform's RAM and is nonpayable to disk. When NT controls a multiprocessor platform, the kernel will run on all processors at the same time and communicate with each other to govern the distribution of threads.

The NT Executive

The NT Executive can be considered a common service provider because it is responsible for providing a set of services to all other operating system components. The Windows NT Executive is the highest level within the kernel mode of the operating system.

As indicated in Exhibit 1, the Executive consists of six core modules that provide an interface between users and computers (represented by Virtual DOS Machines and Environment Subsystems) and the kernel. Virtual DOS Machines support DOS or 16-bit Windows 3.X applications. Windows NT provides support by creating virtual machines and then implementing the required environment within such a machine, resulting in the term “virtual DOS machines.”

In comparison, “environment subsystems” are environments that may be required to operate on top of Windows NT. Examples of currently supported environment subsystems include OS/2, POSIX, and Win32 (the Windows NT subsystem).

Object Manager

The object manager names, retains, and provides security for objects used by the operating system. In a Windows NT environment, an object represents physical items as well as the occurrence of defined situations. Thus, an object can represent directories, files, physical hardware ports, semaphores, events, and threads. An object-oriented approach is used to manage objects. If network managers are using Windows NT, they can view the status of event objects through the NT Event Viewer, which is provided in the operating system as an administrative tool.

Process Manager

In a Windows NT environment, a process represents an address space, a group of objects defined as a resource, or a set of threads. Thus, each of these entities is managed by the process manager. In doing so, the process manager combines those entities into a “virtual machine,” on which a program executes. Here the term “virtual machine” represents a set of resources required to provide support for the execution of a program. Windows NT permits multiple virtual machines to be established, allowing multiprocessing capability.

Virtual Memory Manager

Windows NT uses a special file on the hardware platform's hard disk for additional memory beyond available RAM. That file is referred to as a virtual memory paging or swap file and is automatically created when the operating system is installed.

Previous screen

The Virtual Memory Manager manages the use of virtual memory as a supplement to physical RAM. For example, when one program cannot completely fit into RAM because of its size or the current occupancy by other executing programs, the Virtual Memory Manager might swap one program currently in memory to disk to enable another program to execute, or it could swap portions of the program requesting execution between RAM and the hard disk to execute portions of the program in a predefined sequence.

Although the operation of the Virtual Memory Manager is transparent to programs using it, network managers can change the paging file size. To do so, they would first select the System icon in the Control Panel and then select the Virtual Memory entry from the resulting display. This action results in the display of a dialog box labeled Virtual Memory. Exhibit 2 illustrates the Virtual Memory dialog box with its default settings shown for a Pentium processor.

Virtual Memory Dialog Box

Although Windows NT automatically creates a virtual memory paging file and assigns an initial file size based on the capacity of the system's hard disk, the operating system does not know what applications the network manager intends to run or the size of those applications. Thus, if network managers frequently work with applications that require a large amount of memory, they should consider raising the default setting.

In Exhibit 2, Windows NT provides a pseudo constraint on the sizes of the paging file. That constraint is in the form of a range of values defined for the size of the paging file; however, that range is a recommendation and is not actually enforced by the operating system. For example, to set the initial size of the paging file to two megabytes, the user would type “20” into the box labeled Initial Size and then click on the Set button. Similarly, if users want to raise the maximum size of the paging file to 100 megabytes, they would enter that value in the appropriate location in the dialog box and click on the Set button.

Local Procedure Call Facility

Programs that execute under Windows NT have a client/server relationship with the operating system. The Local Procedure Call Facility is responsible for the passing of messages between programs.

I/O Manager

The Input/Output (I/O) Manager is responsible for managing all input and output to and from storage and the network. To perform its required functions, the I/O Manager uses four other lower-level subsystems—the Cache Manager, file system drivers, hardware device drivers, and network drivers.

The Cache Manager provides a dynamic cache space in RAM that increases and decreases based on available memory. File system drivers provide support for two file systems, the file allocation table (FAT) and the high performance file system (HPFS). The FAT file system provides backward support for DOS and 16-bit Windows 3.X-based programs, whereas the HPFS enables support of the new file system for Windows NT 32-bit applications.

The hardware device drivers used in Windows NT are written in C++ to provide portability between hardware platforms. This allows a driver developed for a CD-ROM, a plotter, or another hardware device to work with all Windows NT hardware platforms.

Previous screen

Network drivers represent the fourth lower-level I/O Manager subsystem. These drivers provide access from Windows NT to network interface cards, enabling transmission to and from the network and the operating system.

The Security Module

Windows NT includes a comprehensive security facility built into the operating system. Once the user turns on power to the hardware platform, this facility is immediately recognizable. Unlike Windows 3.X, Windows 95, or DOS, Windows NT prompts the operator for a password before allowing access to the computer's resources.

Windows NT security works by the log-on process and a local security subsystem that monitors access to all objects and verifies that a user has appropriate permission before allowing access to an object. The log-on process is linked to the Security Reference Monitor, which is responsible for access validation and audit generation for the local security subsystem. Another component of the Security Module is the Security Account Manager. The Security Account Manager maintains user and group information on a secure data base.

Windows NT Networking

One of the biggest advantages associated with the use of Windows NT is its built-in support of many transport protocols. The Windows NT networking architecture was established in a layered design that follows the seven-layer ISOOpen System Interconnection (OSI) Reference Model. Exhibit 3 illustrates the general correspondence between Windows NT layers and OSI Reference Model layers.

Correspondence Between Windows NT and OSI Reference Model Layers

The environment subsystems represent virtual DOS machines as well as 32-bit applications operating on top of NT. At the presentation layer, the Network Provider module is required for each network supported through a redirector. At the session layer, the Windows NT Executive uses a server and redirector to provide capability for a server and workstation, respectively. Both components are implemented as file system drivers and multiple redirectors can be loaded at the same time, so that a Windows NT computer can be connected to several networks. For example, NT includes redirectors for NetWare and VINES, enabling an NT workstation or server to be connected to Novell and Banyan networks.

At the transport layer, the transport driver interface (TDI) provides a higher-layer interface to multiple transport protocols. Those protocols, which represent operations at the network layer, include built-in NT protocol stacks for NetBEUI, used by the LAN Manager and LAN Server operating systems; Data Link Control (DLC), which provides access to IBM mainframes; TCP/IP for Internet and intranet applications; and NWLink, which represents a version of Novell's SPX/IPX protocols. Through the use of TCP/IP, a Windows NT computer can function as a TCP/IP client, whereas the use of NWLink enables a Windows NT computer to operate as NetWare client.

At the data link layer, Windows NT includes a built-in Network Device Interface Specification (NDIS). NDIS enables support for multiple protocol stacks through network interface card drivers. Thus, NDIS allows a network interface card to simultaneously communicate with multiple supported protocol stacks. This means that a Windows NT

Previous screen

computer could, for example, simultaneously operate as both a TCP/IP and a NetWare SPX/IPX client.

Upgrade Issues

The key differences between NT 3.5 and 4.0 are speed and user interface. Windows 4.0 added the Windows 95 user interface to NT. In addition, a recoding of the operating system makes it slightly faster than 3.51. However, because the difference in cost between a Pentium and Pentium Pro microprocessor is a few hundred dollars, it may be more economical to purchase the more powerful processor and retain the familiar Windows 3.51 interface. This could eliminate the costs associated with retraining employees.

Conversely, if an organization has already migrated to Windows 95 or is planning to migrate to that operating system, the network manager may want to consider Windows NT Version 4.0. Its use of the Windows 95 interface may be well known to some or most of the organization's employees who will be using NT, which should minimize training costs while providing a slightly improved level of performance.

Conclusion

The modular design of the Windows NT architecture makes it both portable and scalable. Windows NT's hardware abstraction layer allows the operating system to run on different hardware platforms. Currently, Windows NT runs on Intel X86, Digital Equipment Corp. (DEC) Alpha, MIPS RISC (reduced instruction set computing), and the PowerPC series of microprocessors jointly manufactured by IBM Corp. and Motorola.

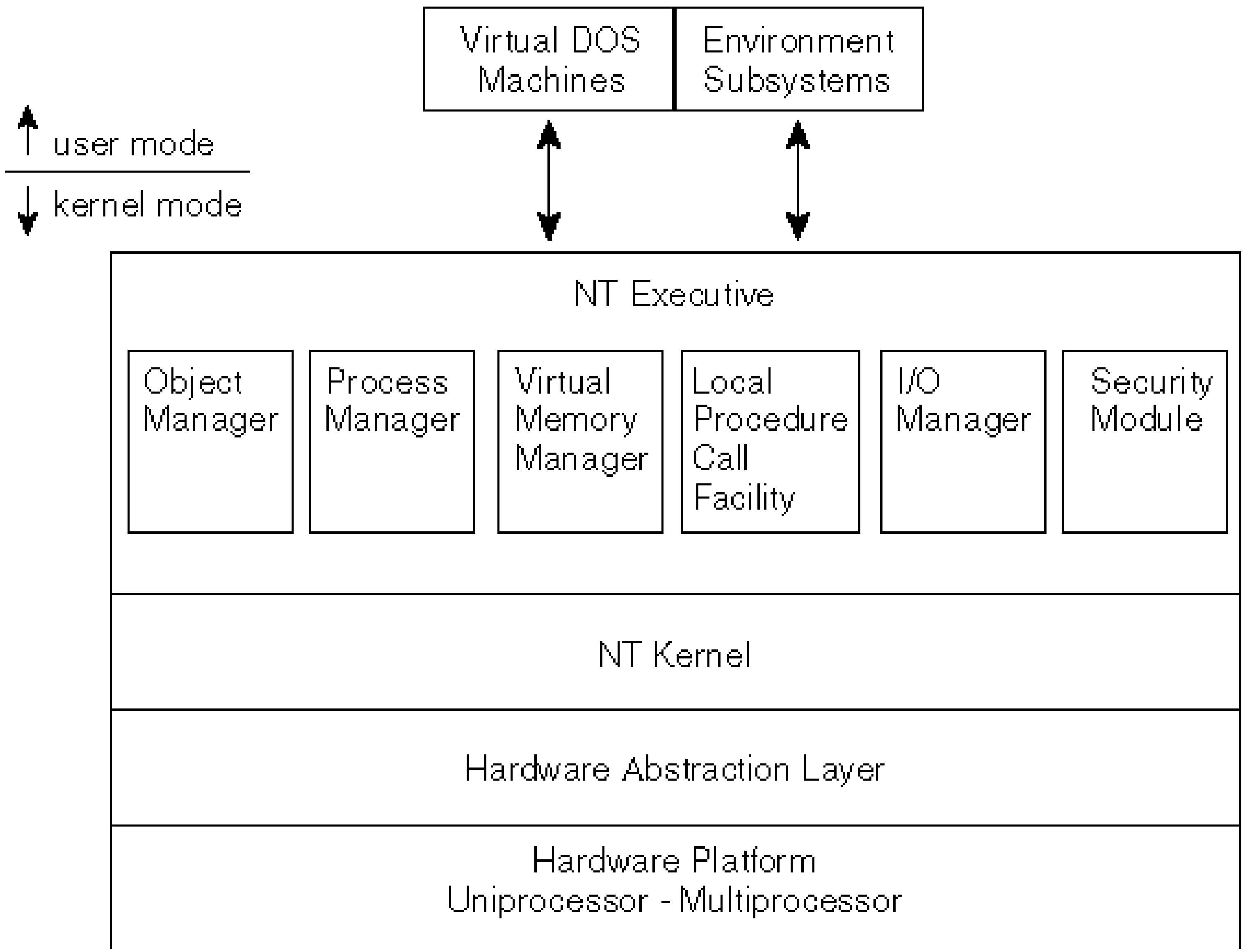
Besides being highly portable, Windows NT supports scalability, which allows the operating system to effectively use multiple processors. Thus, when network managers evaluate Windows NT Server as a platform for different applications, it is important for them to note that they have several options for retaining their investment as applications grow.

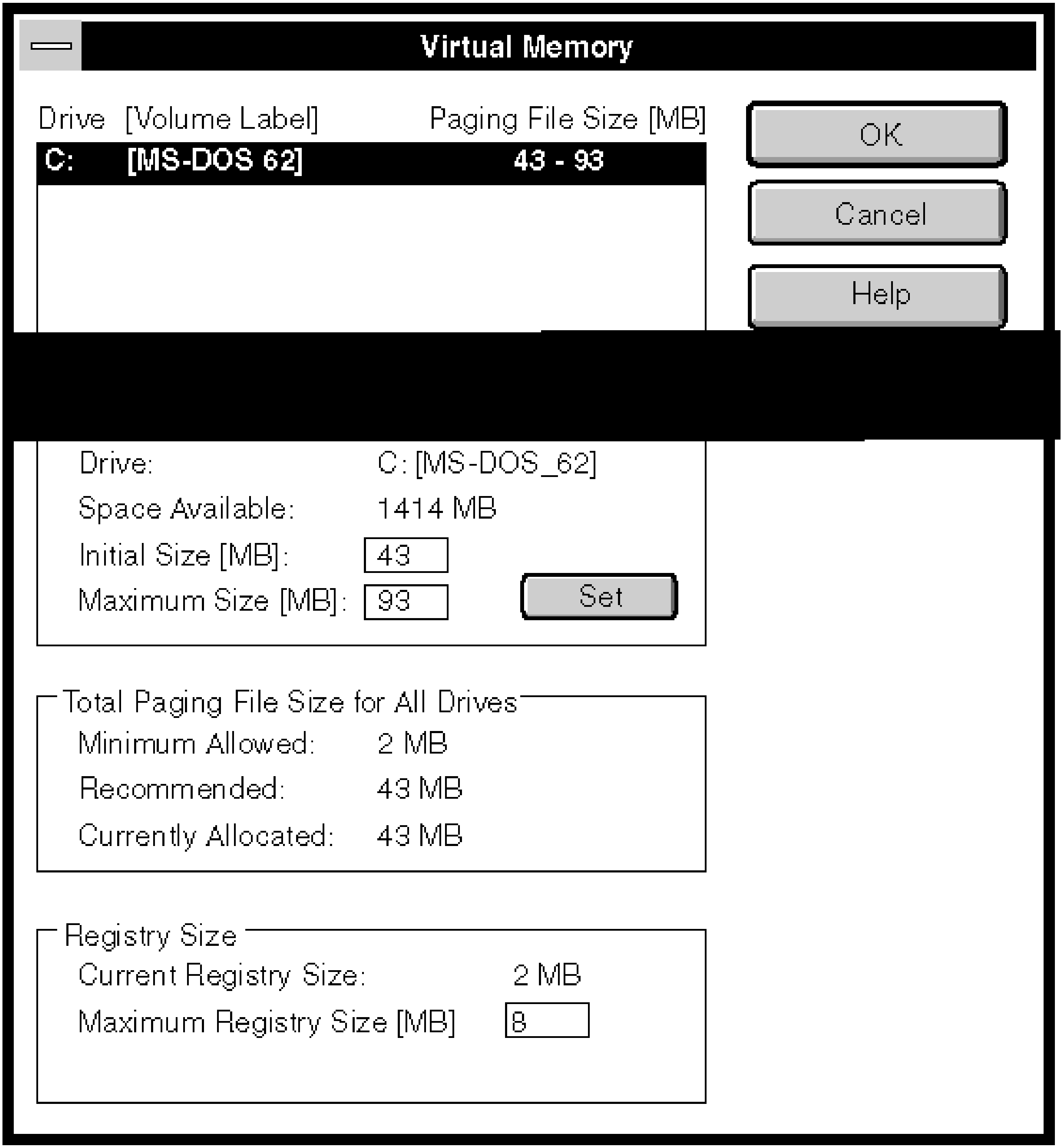
For example, because of its scalability, network managers could replace a uniprocessor Intel Pentium motherboard with a dual- or quad-processor motherboard. If this replacement does not provide the necessary level of processing power, network managers might consider migrating hardware to a high-level PowerPC or a DEC Alpha-based computer. If that migration is required and the applications continue to grow, network managers could use multiple processors to ensure scalability.

Author Biographies

Gilbert Held

Gilbert Held is director of 4-Degree Consulting, a Macon GA-based high-tech consulting group. He is an internationally recognized author and lecturer, having written more than 40 books and 300 technical articles. He earned a BSEE from Pennsylvania Military College, an MSEE from New York University, and MBA and MSTM degrees from The American University. He has been selected to represent the US at technical conferences in Moscow and Jerusalem and has received numerous awards for excellence in technical writing.


Virtual DOS Machines
Environment Subsystems
user mode
kernel mode
NT Executive
Object Manager
Process Manager
Virtual Memory Manager
Local Procedure Call Facility
I/O Manager
Security Module
NT Kernel
Hardware Abstraction Layer
Hardware Platform
Uniprocessor - Multiprocessor



Drive	[Volume Label]	Paging File Size [MB]
C:	[MS-DOS 62]	43 - 93

[redacted]

Drive: C: [MS-DOS_62]

Space Available: 1414 MB

Initial Size [MB]: 43

Maximum Size [MB]: 93

Total Paging File Size for All Drives

Minimum Allowed: 2 MB

Recommended: 43 MB

Currently Allocated: 43 MB

Registry Size

Current Registry Size: 2 MB

Maximum Registry Size [MB] 8

<table>
<tr><th>OSI
Reference Model
Layers</th><th colspan="4">Windows NT Layers</th></tr>
<tr><td>Application</td><td colspan="4">Environment Subsystems</td></tr>
<tr><td>Presentation</td><td colspan="4">Network Provider</td></tr>
<tr><td rowspan="2">Session</td><td colspan="4">Executive Services</td></tr>
<tr><td colspan="2">Server</td><td colspan="2">Redirector</td></tr>
<tr><td>Transport</td><td colspan="4">Transport Driver Interface</td></tr>
<tr><td>Network</td><td>NetBEUI</td><td>DLC</td><td>TCP/IP</td><td>NSLink
(SPX/IPX)</td></tr>
<tr><td rowspan="2">Data Link</td><td colspan="4">NDIS</td></tr>
<tr><td colspan="4">NIC Drivers</td></tr>
<tr><td>Physical</td><td colspan="4">NIC</td></tr>
</table>