Getting Real Advantage from Networking Technology

Microsoft Windows NT Server Network Operating System Version 3.51

Businesses today are changing the way they deal with their networks. In the past, most organizations used their networks primarily as a file sharing and print service. Today, businesses look at their information systems as an investment that gives them a strategic, competitive advantage. The role of the network is shifting from file and print sharing within a workgroup to distributed information systems which support mission-critical business applications. Microsoft® Windows NT™ Server is a robust, multi-purpose foundation that is designed to be both an excellent file and print server as well as a complete, mission-critical applications server.

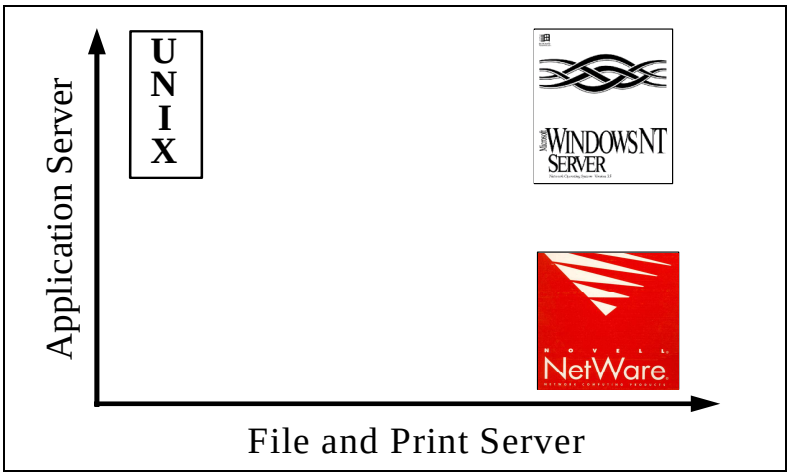

Figure 1: Windows NT Server 3.5 - A Multi-Purpose Server Available Today

As shown above, Microsoft Windows NT Server represents the best of the UNIX® applications servers plus the best of the NetWare file and print servers, all on one platform. Windows NT Server is today's—and tomorrow's—networking foundation.

Businesses are ready to make this investment in infrastructure, hardware, and software. As Jamie Lewis of The Burton Group puts it, "It's already common for organizations to implement mission-critical databases on network servers, some of which run on minicomputer-scale hardware."[1] In order to remain competitive, other businesses need to understand what these companies already know: *the real advantage of distributed information systems supporting mission-critical business applications on network servers*. The purpose of this paper is to discuss the features of a truly useful and effective distributed information system, and how Microsoft Windows NT Server is the best network foundation for distributed systems.

THE FEATURES OF AN EFFECTIVE DISTRIBUTED SYSTEM FOUNDATION

The proliferation of personal computers has created tremendous computing power and computer-based data in today's organizations. By connecting all of these individual machines in new ways, it is possible to maximize their use and effectiveness. Such "distributed systems" make it possible to share information easily, yet securely. In addition, new distributed applications can be deployed, which give users access to critical information more easily and effectively than ever before. This results in better decision-making, thus enabling companies to give better service to their customers. Of course, the bottom line benefits of distributed systems will only be realized if administrators can easily and cost-effectively manage these vast collections of individual machines.

There are several important features required to bring distributed collections of computers together into a powerful and manageable unit. The distributed system must offer:

[1] *Burton Group Report—Network Operating Systems: NT Server 3.5;* February, 1995, p. 1.

- Basic file and print services.
- Comprehensive support for mission-critical applications.
- Ease of installation, system management, and use.
- Easy integration and interoperability with existing systems.
- The ability to readily incorporate new technology as it becomes available.

Windows NT Server offers all of these features. It is a robust, multi-purpose network operating system that provides both high-performance file and print services, and the infrastructure to run powerful client-server applications.

COMPREHENSIVE SUPPORT FOR BASIC NETWORK SERVICES AND MISSION-CRITICAL APPLICATIONS

Organizations today use network technology in a number of different ways. Networks connect users to file servers, printers, mainframe systems, mid-range application servers, messaging systems, and a variety of other services. The problem, however, is that all of these services usually run on different systems. An organization might use Novell® NetWare® for its file and print services, UNIX or AS/400 systems for mid-range database and messaging applications, and mainframes for centralized, business-critical applications. This collection of disparate systems can be difficult to integrate, difficult to use, and difficult to manage.

Windows NT Server is designed to provide comprehensive support for all of these different services on a single, easy-to-manage platform. It takes advantage of the increasing power and decreasing cost of microprocessor-based computers to provide powerful, cost-effective computing solutions that meet changing business needs. In addition, Windows NT Server integrates smoothly into today's network environments, adding substantial value and capability, while preserving the investments customers have made in their existing technology.

In order to provide effective support for all of these different network services on one, multi-purpose platform, Windows NT Server was built on a fully 32-bit microkernel foundation. It is multithreaded, offers preemptive multitasking, and provides memory protection for both applications and the operating system itself. It scales to run on hardware with up to 32 processors, 4 GB of RAM, and 402 million terabytes of disk space. In addition, Windows NT Server supports Intel® x.86, MIPS® R4x00, DEC® Alpha AXP™, and IBM® PowerPC™ processors. As a result, Windows NT Server provides all the components necessary to support both basic network services and mission-critical applications, including:

- High performance file and print services
- Excellent applications server performance
- Excellent balance between its central management capabilities and user autonomy so that individual users can have some control over the resources they own while maintaining network security
- The robustness necessary to support mission-critical applications and tolerate individual application or system faults
- High availability of user services
- A secure environment that prevents unauthorized access to information
- The ability to scale and support a very large numbers of users
- Complete integration with Windows® 95

High Performance File and Print Services

File and printer sharing is a basic network service that virtually all users require. One way of measuring file and print service performance is to use independent third party benchmark tests, such as Netbench 3.0.

Netbench 3.0 is a Ziff-Davis benchmark that is used to measure file input-output performance for different network operating systems. It is designed to test file services and is network operating system independent. It does not measure application server performance (Serverbench is the test used for this purpose; see next section). Netbench 3.0 clients send out requests to a network server which then processes these requests. Netbench 3.0 does not use real applications; it is a synthetic test that models real application behavior.

As the following NetBench 3.0 graph shows, Windows NT Server 3.51 provides file and print service comparable to NetWare 4.1. This test was run on a uni-processor Compaq® Computer Corp. ProLiant™ P100, with 128M bytes of RAM, 6x2G byte hard-disk array, and four Netflex 2 Ethernet network interface cards. Each of the operating systems was tested with one to 48 clients running against the server.

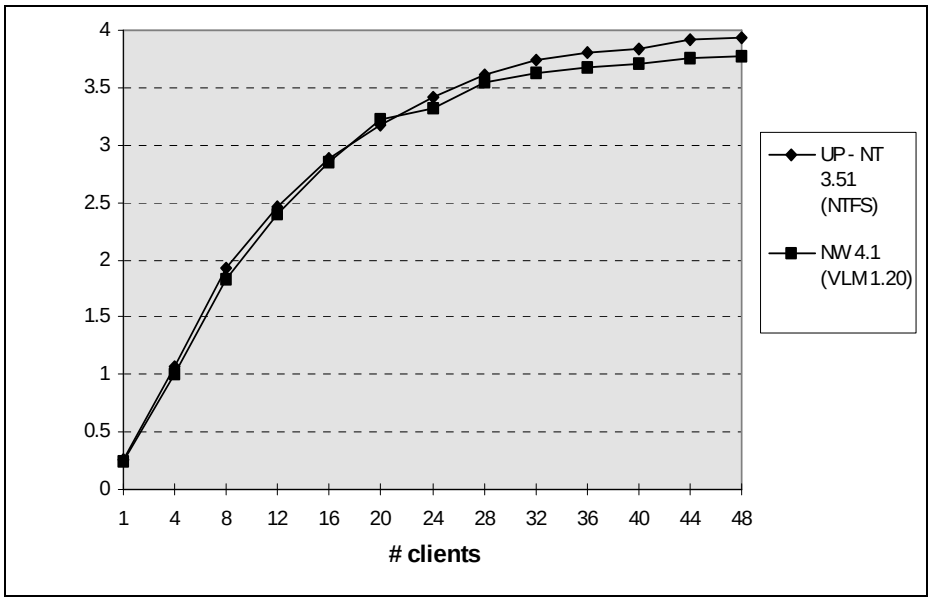

Figure 2: Netbench 3.0 Test Results - File and Print Service Performance

Windows NT Server provides excellent file and print service, more than keeping pace with NetWare 4.1. In fact, as the number of clients increases, Windows NT Server 3.51 actually provides better file and print service, peaking at nearly 4 Mbytes/sec with 48 clients, than NetWare 4.1, which peaks at nearly 3.8 Mbytes/sec with 48 clients.

Excellent Applications Server Performance

As a foundation for mission-critical, client-server business applications, Windows NT Server was designed to provide excellent applications server performance. As with file and print service performance, applications server performance is typically measured using a third party benchmark test. In this case, the test is Ziff-Davis' Serverbench 2.0.

Serverbench is a true client-server application that runs on NetWare 3.12, SCO UNIX, and Windows NT Server 3.5. An application optimized for each of these operating systems runs on the server and the clients run a set of predefined tests. This is different from Netbench, which is operating system independent.

Serverbench measures the performance of the processor, disk, and network subsystems by running different types of tests that produce different loads on the server. Serverbench is an excellent measure of the real world because it simulates how real users use the network operating system as both an application server and file server. This test shows results in transactions per second (TPS).

The following graph shows the Serverbench results in a multi-processor test with Windows NT Server 3.5 (2 and 4 processors), SCO UNIX (2 and 4 processors), and NetWare 3.12 (1 processor only). These results were published in *PCWeek;* the graph is a compilation of the available data. NetWare 3.12 is shown on this graph by way of comparison, despite the fact that it can only run on a single processor machine. This test was run on a Compaq Computer Corp. ProLiant 4000, with 128M bytes of RAM, 6G bytes of hard-disk space, and four Compaq Netflex 2 EISA Ethernet network interface cards. Each of the operating systems was tested with one to 60 clients running against the server.

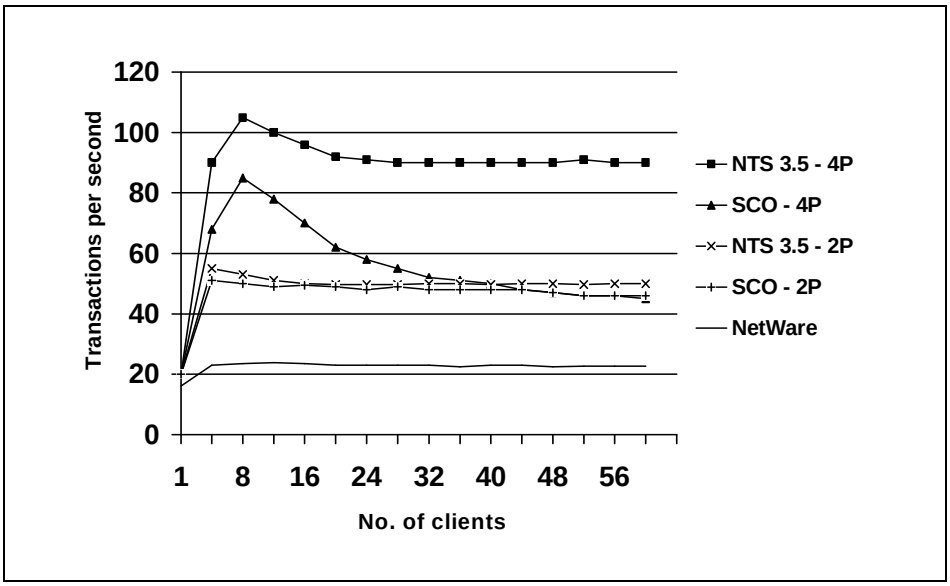

Figure 3: Serverbench 2.0 Test Results - Applications Server Performance

As this graph clearly shows, Windows NT Server 3.5 is an extremely fast client-server platform and shows near-linear scalability as processors are added. Windows NT Server peaks at more than 100 tps with four processors, whereas SCO peaked at nearly 20 tps lower. SCO performance also dropped off significantly when the number of clients exceeded 20. Windows NT Server is clearly the fastest multi-processor networking platform available.

User Autonomy

User autonomy means that individual users maintain control of their own resources within the security context of the distributed system. For example, with a Windows NT Server-based network, a user can create a directory to share files with co-workers. That user can then control who accesses that directory by specifying the directory's user access rights using Windows NT Server's directory services.

The following illustration shows how a user sets the access rights for a directory called "budget."

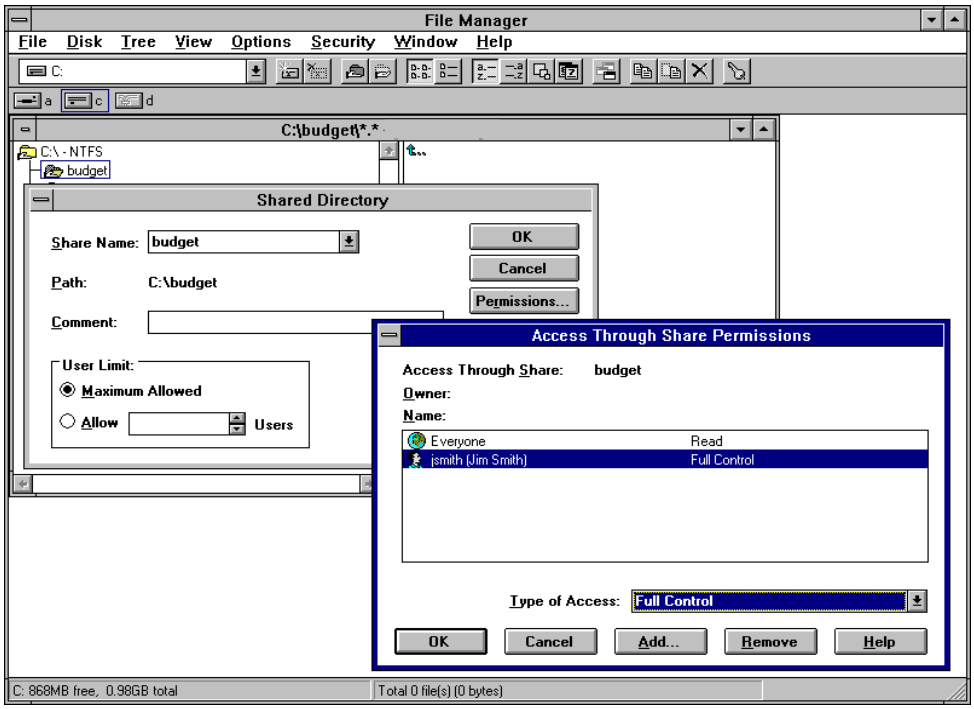

Figure 4: Setting access rights for users

The owner of "budget" assigns access rights to users with user accounts in the network's central user database. In other words, suppose Jim wants to store data in "budget" but only wants everyone else to be able to read the data. Jim simply assigns "Everyone" read-only access to the directory "budget" and retains "full control" for himself. This means that Bob, for example, can only read files from the directory "budget." Jim, however, can read, write, delete, create, and change files in the directory "budget."

Assigning access rights in this manner lets "budget's" creator control who can access the directory and how they can access it. However, it does not require separate user accounts on "budget's" server. Instead, "budget's" owner assigns rights to network users whose accounts are maintained and authenticated centrally. As a result, the owner's freedom to control the resource is preserved while overall system security is maintained. The central administrator also benefits in that, while maintaining security, simple file sharing rights can be allocated to the file owners. The administrator is then free to attend to more pressing issues, rather than whether someone can read Jim Smith's budget report, for example. Jim Smith can determine who reads his document. This user autonomy is applicable to any resource a user may own and wish to share including files, servers, directories, printers, and other peripherals. It also means that Windows NT Server provides excellent balance between its central management capabilities and user autonomy. This balance translates into more efficient ways to handle information, as well as better access to that information, on a company-wide scale.

Robustness and High Availability of User Services

Reliability is a key component in today's network. One of the most powerful characteristics of the Microsoft Windows NT Server operating system is its reliability. Built into every component of Windows NT Server, reliability provides maximum availability of information and services to users. The system ensures this high availability in a number of ways, including:

- uniformly handling hardware and software system faults
- protecting user programs from each other as well as the system
- providing data and system recovery mechanisms.

By building reliability technology into Windows NT Server from the start, we have ensured the system's ability to tolerate faults while still maintaining the availability of the system, applications, network resources, and data. Further, Windows NT Server's microkernel construction means that it is easy to add new services and features, without disrupting existing ones.

Windows NT Server includes the following reliability and fault tolerance capabilities:

- **Error handling and protected subsystems.** Windows NT Server is designed to gracefully manage application and system errors and exceptions, without bringing down the system. Also, protected subsystems isolate programs in unique memory locations to ensure that one program's fault will not affect the operation of other programs or the system.
- **Recoverable file system.** The Windows NT file system (NTFS) is highly tolerant of disk failures because it logs all disk I/O operations as unique transactions. In the event of a disk failure, the file system can quickly undo or redo transactions as appropriate when the system is brought back up. This dramatically reduces unavailable time since the file system can return to a known, functioning state quickly.
- **Automatic restart.** Windows NT Server's error handling and protected subsystems make system failures extremely rare. However, if a failure does occur, the system can be set to restart itself automatically. This feature provides maximum unattended uptime. In addition, memory contents can be written to a disk file prior to the restart to assist the administrator in determining the cause of the failure.
- **Tape backup support.** Windows NT Server includes powerful tape backup to ensure data availability. Third party backup products are also available from vendors such as Arcada and Cheyenne.

- **Uninterruptible power supply (UPS) support.** The UPS service for Windows NT Server detects and warns users of power failures and manages a safe system shutdown before the backup power supply is exhausted.
- **Disk mirroring, disk duplexing, and disk striping with parity (RAID 5).** These are all methods of creating data redundancy by duplicating it on other partitions. Each method provides a different level of fault tolerance. Similarly, each method has different costs associated with it. Windows NT Server includes each of these methods so users may choose the combination of price and fault tolerance that best suits their needs.

The net result is that Windows NT Server is the most reliable foundation available, one that is designed to work as well with tomorrow's technology as it does with today's. For more information on Windows NT Server's reliability and fault tolerance capabilities, please refer to the Microsoft Windows NT Server Technology Brief *Reliability and Fault Tolerance*.

A Secure Environment

Windows NT Server was also designed from the ground up to be extremely secure. Security features are built into every component of the operating system and are designed to meet the U.S. Department of Defense's National Computer Security Center's (NCSC) requirements for a C2 certifiable secure system. In addition to the U.S. government's requirements, Windows NT Server solves numerous "real world" security problems. These include ease of use by end users and ease of management by network administrators. Windows NT Server is even designed to protect data stored in a computer's memory so it cannot be accessed by another, unauthorized process.

This means that, for example, Jim Smith must logon and be validated by the system in order to gain access to data. Further, he must be given explicit access to data on the system or he will not gain access to it. While Jim only sees the security features when he logs on, he is constantly being validated by the system every time he tries to access data. This detailed attention to security helps ensure that information is fully protected and accessed only by authorized users.

Building a secure network operating system required careful planning. Security features must be included throughout the system. The file system, user account directory, user authentication system, memory management, environment subsystems, and other components all require special design consideration if the system is to be secure. Microsoft made security a design goal of the Windows NT operating system. Before the system was built, security features were designed into every facet of the operating system. This early planning and design was critical to the successful development of a secure system and ensures Microsoft's continuing ability to provide comprehensive, usable security in Windows NT Server. Windows NT Server's security is yet another aspect of its reliability.

For more information on Windows NT Server's security features, please refer to the Microsoft Windows NT Server Technology Brief *Security*.

Scalability

The Microsoft Windows NT Server operating system offers a truly scaleable platform on which to build business solutions. This scalability means that Windows NT Server-based applications can meet the changing needs of small, medium, and large organizations by running on a broad range of hardware—from machines with one processor and 16 megabytes of memory to machines with 32 processors and 4 gigabytes of memory. And Windows NT Server can operate on Intel x.86, MIPS R4x00, DEC Alpha AXP™, and IBM PowerPC™ processors.

By running on such a broad set of hardware, Windows NT Server-based solutions grow with an organization. Hardware power can be added to an existing software solution, resulting in increased capacity and performance, with no changes to the application's operation or management. Similarly, by deploying Windows NT Server-based solutions consistently throughout an organization, the different groups within that organization can readily share information and benefit from consistent, easy-to-use application interfaces.

Windows NT Server has been deployed successfully in many large customer sites, often demonstrating tremendous scalability. For example, Bell Atlantic recently migrated their budgeting process from mainframe-based IMS/Focus applications to a more flexible and

responsive system based on Microsoft SQL Server. The system supports users with databases replicated over several sites. The largest sites have AT&T® GIS 3455 SMP servers with six 90mhz Pentium processors and 40-gigabyte RAID arrays. The current deployment extends to 8 servers and 420 clients and will ultimately include 19 servers and more than 1,000 clients.

Reliability, fault tolerance, security, and scalability: the four pillars upon which Windows is built. Windows NT Server is the right long-term networking choice.

For more information on Windows NT Server's scalability, please refer to the Microsoft Windows NT Server Technology Brief *Scalability*.

EASE OF INSTALLATION, MANAGEMENT AND USE

By their very nature, distributed systems are made up of many individual machines distributed throughout an office, region, country, or the world. While such a configuration can dramatically improve information access and organizational response time, it can also be difficult and expensive to manage. In order to help lower the network management and support burden, Windows NT Server includes a number of utilities designed to make the installation, administration, and use of a Windows NT Server-based network easy and straightforward—benefits that result in more efficient use of time and financial resources.

Installation

Networks today are plagued by operating systems that can be difficult to install and configure. As a result, Microsoft has included the following features in Windows NT Server to dramatically reduce setup time:

- **CD ROM-based ExpressSetup and hardware autodetect.** Quickly installs Windows NT Server program files onto the server's hard drive. ExpressSetup prompts the administrator for basic parameters such as computer name, choice of file system, and number of client access licenses. Installation procedure permits user review and configuration of all network protocols and services.
- **Hardware autodetect.** Disk drives, video card, network interface card, sound system, and other hardware devices are automatically detected and drivers are automatically installed.
- **Script support.** Allows for automated setup and unattended installation.
- **Network Client Administrator.** Allows for automatic, "over-the-network" installation of network client software, including Windows® for Workgroups and Windows 95.
- **All components included.** Windows NT Server ships with all protocols (TCP/IP, IPX/SPX, NetBEUI, AppleTalk®, SNA DLC), Remote Access Service, Macintosh® connectivity, Telnet and FTP clients, FTP server, and management utilities. All the components you need for your network are right in the box.

By including these components and utilities with Windows NT Server, installation time is typically completed in minutes rather than hours. As a result, Windows NT Server setup is significantly faster and easier than today's UNIX and NetWare operating systems. And, because Windows NT Server is so easy to set up, you spend less time and resources installing your network and more time being productive.

Management

Another key component of Windows NT Server is its central management capabilities. Managing a network can be both expensive and time-intensive. Administrators can spend much of their time simply trying to track down problems with the network rather than being productive.
Windows NT Server provides central management, relieving the often tremendous burden on the administrator. Once Windows NT Server is installed, maintaining your Windows NT Server-based network is done with a series of graphical network management tools included with the operating system. These utilities, depicted in the following illustration , offer a comprehensive set of management functionality.

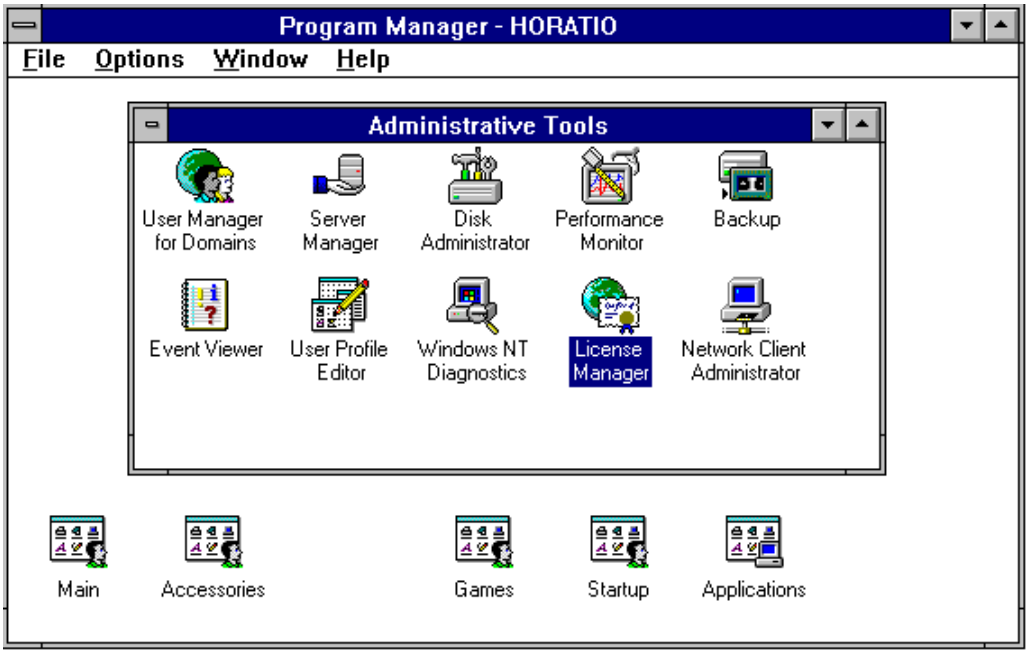

Figure 5: Windows NT Server Administrative Tools

Each utility allows for management and monitoring of network resources and performance. In most cases, the utilities can be run from any Windows NT Server, Windows NT Workstation, Windows, or Windows for Workgroups-based computer on the network. They can also be operated from a remote computer connected via a standard phone line, X.25, or ISDN link. Regardless of where the tools are used, they provide centralized monitoring and management of network resources, essential aspects of today's demanding networks. Windows NT Server's management tools include:

- **User Manager.** Used to add, delete, and modify user and group accounts for the entire network. Users access rights can be easily modified via simple "drag and drop" operations. Logon hours, logon workstation, group memberships, user profiles, password aging, and numerous other parameters are configured with User Manager.
- **Server Manager.** Monitor the users, sessions, shares, files in use, and alert conditions for any Windows NT Server or Windows NT Workstation on the network. Also used to configure directory replication.
- **Disk Administrator.** Manage disk volumes and partitions, configure mirrors, duplexes, and stripe sets. Format drives and regenerate stripe sets when required.
- **Performance Monitor.** Graphically displays performance information for 400-plus network and server parameters. Processor utilization, network utilization, application transactions per second, disk read/write times, paging file usage, and numerous other parameters can be monitored. This information can be used to prevent system bottlenecks and load balance.
- **Backup.** Used to backup and restore files to tape devices. Backs up local and remote files, directories and volumes. Supports FAT, HPFS, and NTFS file systems. Offers normal, copy, incremental, differential, and daily backups. Batch files can be used to automate repeated backups.
- **Event Viewer.** Allows the administrator to view all events recorded in event logs. Event types include system, application, and security events. The event logs provide detailed information on all system activities and can be used to track any anomalies or system problems.
- **User Profile Editor.** Used to create and edit individual user workstation configuration information. User profiles configure desktop arrangement, personal program groups, screen colors, network connections, printer connections, mouse settings, and window size and position. User profiles can be stored on authenticating servers so that users can access the

same profile regardless of logon location. User profiles help reduce the administrative overhead associated with user workstation configuration.

- **Windows NT Diagnostics.** Provides detailed information about the operating system version, server hardware, memory, drivers, services, devices, IRQ and port status, DMA/Memory status, environment variables, network status, and drives. Diagnostic tools including the Disk Administrator, Event Viewer and Registry Editor can be activated.
- **License Manager.** Used to track Microsoft Client Access Licenses. Parameters include purchase history, quantity of valid licenses, licenses in use, products licensed, and licensed users.
- **Network Client Administrator.** Automates Windows NT Server client software installation. The Network Client Administrator enables the network manager to create a single "boot" floppy for client workstations. Upon boot up with this floppy, the client computer is automatically connected to a Windows NT Server and appropriate client software is installed. Client software installation options include MS-DOS®, Windows for Workgroups, and Windows 95. All client software is shipped with Windows NT Server. Client software licenses, such as for Windows for Workgroups or Windows 95, must be purchased separately.

The ease of central management provided by Windows NT Server directly affects the bottom line: the less time an administrator has to spend tracking down and fixing the problems of a network, the better the productivity.

Managing TCP/IP

Windows NT Server also includes functionality designed to ease the management burdens associated with TCP/IP. The Dynamic Host Configuration Protocol (DHCP) is a method of automatically assigning IP addresses to individual network nodes, designed because manual assignment requires substantial administrative time and is often subject to error. The goals of the TCP/IP projects at Microsoft are: to provide 32-bit performance, provide ease of configuration that users have today using NetBEUI or AppleTalk®, and to provide ease of administration by using a dynamic and scaleable TCP/IP addressing capability. Also, Microsoft has ensured that no workstation configuration would be necessary, and that users do not need to know anything about a computer's TCP/IP address. To meet these goals, Microsoft developed DHCP.

TCP/IP is a widely accepted, routeable, WAN protocol that is unparalleled in its deployment worldwide as a de facto standard for wide-area networking. It is also the language of the Internet, making it a highly desirable protocol for the desktop environment. But, until the advent of DHCP, TCP/IP had been inherently difficult to use and manage. Every computer running TCP/IP must have specific information to uniquely identify itself, the network that it is a member of, and the location for packets not bound for computers on the local network. This information is referred to as the TCP/IP address, subnet mask, and default gateway, respectively. Each of these addresses consists of a 32-bit number usually represented in dotted decimal format. For example, in a typical TCP/IP configuration, the TCP/IP address might be 101.200.42.101, the subnet mask 255.255.0.0, and the default gateway 101.200.42.1.

Such requirements can create serious administrative difficulties in large network environments. For example, suppose a department orders a new computer and it comes with all of the necessary software and hardware preinstalled to connect to the corporate network. However, the computer cannot be attached to the network, nor can it access any TCP/IP-based network resources, until the network administrator provides the necessary client information. Furthermore, either a person from the "helpdesk" needs to physically go to the computer to enter the appropriate information or the user needs to dig through documentation and figure out how to do it himself. The key factor here is the ability of the user to enter the necessary client information correctly versus having a technician enter the information at a high hourly rate.

Complex TCP/IP addresses are not only difficult to manage, they are difficult to use. If a user needs to access information located on a network node other than his own, the user typically refers to that computer by its name, not its TCP/IP address. This is because a computer name, like "FINANCE," is much easier to use than a complex TCP/IP address. When the user refers to

this name, the system then accesses a host table that contains a mapping between the computer's name and it's TCP/IP address.

The difficulty of the host table lies in its administration. It is a static document that requires manual maintenance and updates each time network nodes are added or moved. For typical clients using services such as NFS, the host table resides on local computers. This means that either the users need to know enough about host files and TCP/IP addresses to update the host table information themselves or the administrator needs to maintain the information on a server and periodically download the updated file to the client machines.

Some organizations implement the Domain Name System (DNS). DNS keeps the host table on a server. Users only need to specify the address of the DNS server on their local machine. However, DNS does not alleviate the need to update the host table information manually. Although DNS is server-based, it is not dynamic and must be manually updated whenever a computer name or TCP/IP address is changed.

Microsoft implemented DHCP, a protocol developed in conjunction with the Internet Engineering Task Force, in Windows NT Server version 3.5. Using DHCP, the administrator specifies a range, or *scope*, of IP addresses on the server. Addresses are then automatically assigned, or *leased*, to individual nodes when those nodes connect to the network. Administrators no longer need to enter a unique IP address at every node machine. Additionally, DHCP prevents the assignment of the same IP address to more than one node. Finally, DHCP helps conserve IP addresses because they are leased to network nodes. If a particular node no longer needs its IP address, the address can be leased to a different node. DHCP alleviates the burden on the administrator, freeing time for other, more productive tasks. The implementation of DHCP in Windows NT Server is another example of Microsoft's focus on ease and cost of management.

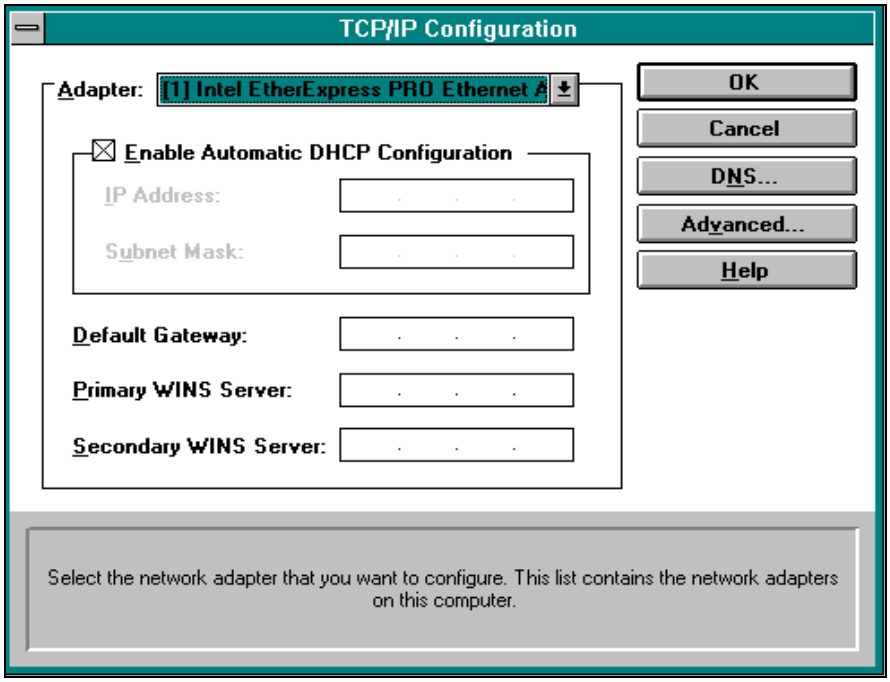

Figure 6: TCP/IP configuration using DHCP

This screen above is a view of the client-side configuration of TCP/IP using DHCP. When configuring TCP/IP for the first time, the client clicks on the button "Enable Automatic DHCP Configuration," thereby enabling that local machine to go and find a DHCP server and automatically get a TCP/IP address. The user never needs to know what the TCP/IP address is and, every time the user boots that local machine, it will be automatically assigned a valid TCP/IP address by a DHCP server.

The following screen is a view of the DHCP server itself. As you can see, DHCP allows the administrator to choose a scope of addresses from which a local machine will be automatically assigned a TCP/IP address, exclude certain addresses and scopes, and limit the duration of the

TCP/IP lease. The DHCP server also prevents two machines from being given the same TCP/IP address. All this means that the administrator no longer needs to worry about TCP/IP address conflicts and is spared the task of allocating a specific address to a specific machine every time that machine is booted. It also means that the end-user is spared having to know anything about TCP/IP addresses and their management.

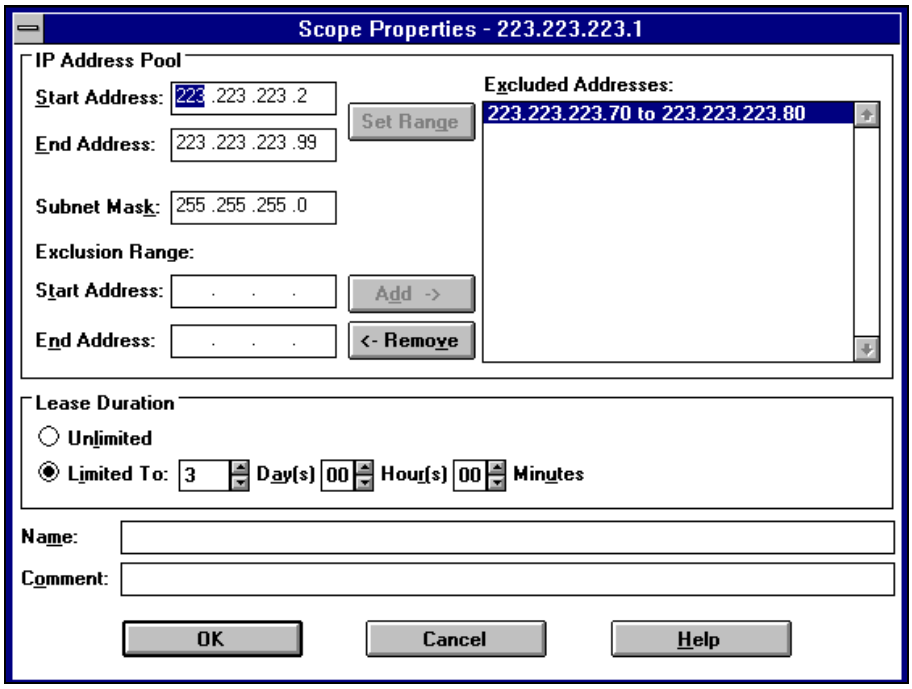

Figure 7: DHCP Server

Effective use of TCP/IP further requires mapping the "friendly" machine name of each network node to it's IP address. This mapping, or name *resolution*, allows both users and applications to refer to nodes by their friendly names instead of their more complicated IP addresses. Today, name resolution is usually accomplished using "host" files. Host files contain the names and IP addresses of IP network nodes. The problem with host files is that their entries are static; changes or additions to the name/address mappings must be made manually by the administrator.

In order to allow for dynamic mapping of machine names to their IP addresses, Microsoft also implemented the Windows Internet Name Service (WINS) into Windows NT Server 3.5. WINS maintains a database that maps each machine name to its IP address. The benefit of WINS is that changes, additions, or deletions to the mapping information are automatically made to the WINS database. For example, if a DHCP server leases an IP address to a new network node, that address and the node's name are automatically entered into the WINS database. Network services that use machine names can now rely on WINS to resolve the names with their IP addresses. The administrator is not forced to manually update host mapping files, thereby reducing both administrative overhead and the opportunity for entry errors. The following screen is a view of the WINS database that indicates all of the mappings, the TCP/IP addresses, and their expiration dates.

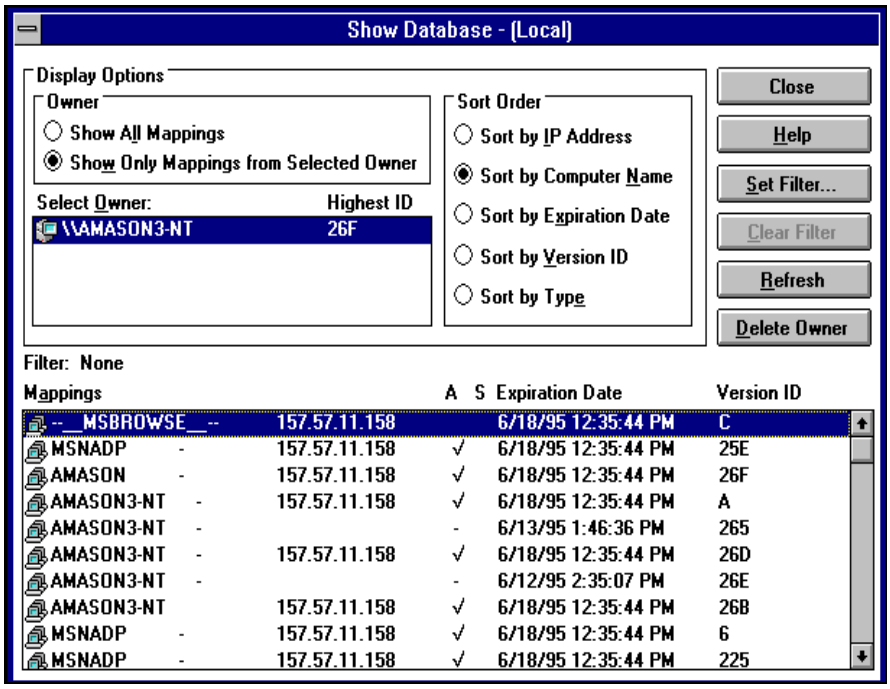

Figure 8: WINS database

Both DHCP and WINS are important elements of Microsoft's effort to make networking with TCP/IP a practical reality. Like the other management tools offered in Windows NT Server, these features work together to make networking with Windows NT Server easy and cost-effective.

For more information on DHCP and WINS, please refer to the Microsoft whitepaper, *Dynamic Host Configuration Protocol and Windows Internet Name Service* and the Microsoft Technology Brief, *Protocols*.

INTEROPERABILITY WITH EXISTING SYSTEMS

Many organizations today use a variety of networking technologies to share information and resources among users. These organizations have made significant investments in their networking technology and want to be sure that new technology can be easily integrated into existing environments. Windows NT Server is designed to interoperate with many of today's most common network systems. As a result, users can continue working with the systems they know while gaining the added benefits Windows NT Server has to offer.

Windows NT Server works with the following:

- Novell NetWare
- Microsoft Windows for Workgroups
- AppleTalk
- DEC PATHWORKS™
- IBM LAN Server
- IBM SNA networks
- Microsoft LAN Manager
- NFS networks
- Remote access services via ISDN, X.25, and standard phone lines
- TCP/IP networks, such as UNIX-based networks
- The Internet

Integrating with Novell NetWare

Windows NT Server can add substantial value to a Novell NetWare network. Its robustness, high-performance file and print services, powerful applications support, remote access

capabilities, ease of use, and integration with the Windows family of desktop operating systems, make Windows NT Server an excellent addition to an existing NetWare network. Windows NT Server supports numerous Services for NetWare that enable it to fully integrate with today's NetWare networks without modifying any of the client-side software. These services enable:

- Existing NetWare clients to access Windows NT Server file, print, and application services.
- Microsoft network clients to access NetWare file and print servers.
- NetWare 2.*x* and 3.*x* binderies to be centrally managed using Windows NT Server Directory Services and administration tools.
- A smooth integration and migration of NetWare servers to Windows NT Server using the Windows NT Server Migration Tool for NetWare.

Windows NT Server provides connectivity in NetWare environments by supporting both the IPX/SPX transport protocol and the NetWare Core Protocol (NCP) file and print service protocol.

Accessing Windows NT Server-Based Applications from NetWare Clients

Windows NT Server provides NetWare client access to Windows NT Server-based applications, such as SQL Server databases or SNA Server host connectivity. NetWare clients can thereby benefit from Windows NT Server's applications, without having to change the client-side software. This is accomplished via the IPX/SPX protocol and client-side code that provides an interprocess communication protocol (IPC) for the applications on top of the IPX/SPX protocol. The IPX/SPX protocol ships with Windows NT Server and the client side IPC code ships with individual server applications such as Microsoft SQL Server and SNA Server. This simple solution further supports easy integration of Windows NT Server-based computers into a NetWare environment.

The following screen is a view of an integrated Windows NT Server and NetWare network with the IPX/SPX protocol stack deployed.

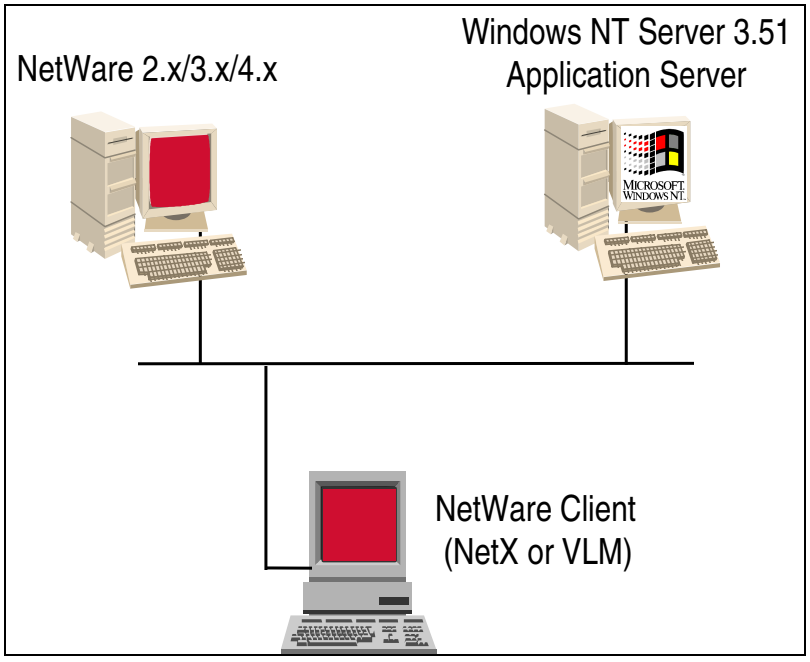

Figure 9: NWLink, the IPX/SPX-compatible transport

Accessing Windows NT Server File and Print Services from NetWare Clients

Today's NetWare clients, such as Windows-based computers running Novell's NetX or VLM client software, can also easily access Windows NT Server-based file and print services. This

access is enabled by a new Windows NT Server utility called File and Print Services for NetWare (FPNW).

File and Print Services for NetWare is a Windows NT Server utility that makes Windows NT Server look like a NetWare 3.12 compatible file and print server. With File and Print Services for NetWare, customers can deploy basic NetWare file and print services, as well as powerful, advanced business applications on the same Windows NT Server-based machine, without changing their client software.

For example, suppose Jim Smith would like to migrate his network from NetWare to Windows NT Server because he wants both a file and printer server and an application server. The problem is that he has 1,000 clients and migrating would mean that he has to change all of the client software at the same time. By installing FPNW on a Windows NT Server-based machine, the NetWare-based clients can access the Windows NT Server for file and print services, as well as its applications, and it will look to them as though they are accessing a NetWare server. Jim can then change his client-side software when he has time, and when he can afford to.

FPNW also gives the NetWare client greater capability. For example, when a NetWare client sends an NCP file access request or print job to a Windows NT Server-based computer running FPNW, FPNW interprets the request and responds appropriately. If proper user access rights exist, an NCP encoded response is sent to the file request. Similarly, print jobs are sent to the correct print queue. FPNW is an excellent option for NetWare sites wanting to deploy Windows NT Server without simultaneously modifying the client software and all of their NetWare client machines.

Deploying FPNW on Windows NT Server-based machines allows the administrator to take advantage of central administration of NetWare client user accounts while NetWare clients enjoy a single logon to all network file, print, and application service resources.

The following screen is a view of FPNW deployed in an integrated Windows NT Server and NetWare network.

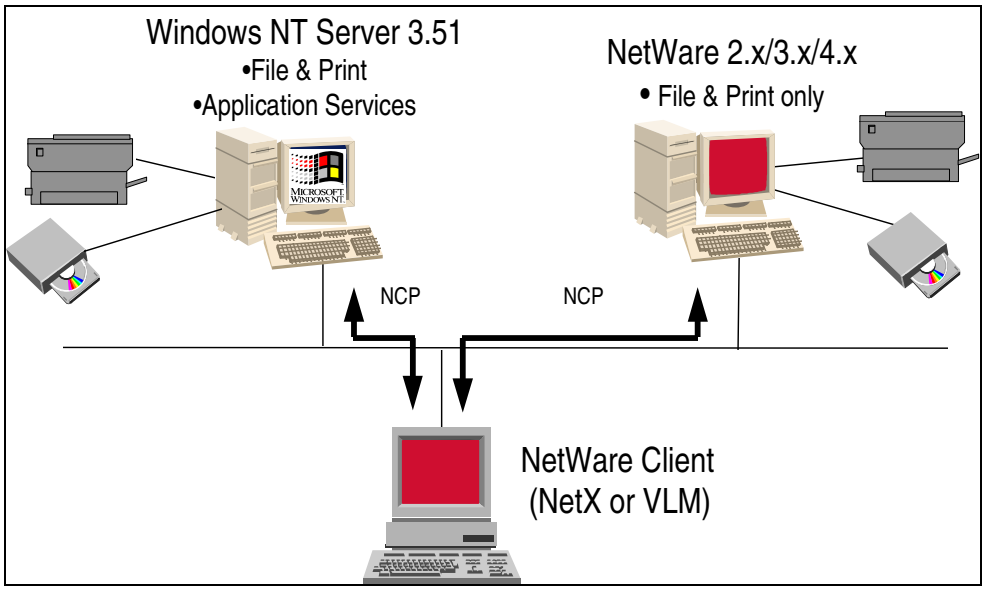

Figure 10: File and Print Services for NetWare

Accessing NetWare File and Print Services from Microsoft Clients

Most newer Microsoft client software, including Windows for Workgroups 3.11, Windows NT Workstation, and Windows 95, support direct NCP connections to NetWare file and print services via the IPX/SPX transport protocol. However, older Microsoft client software for MS-DOS and Windows only support Microsoft's Server Message Block (SMB) file and print service

protocol. As a result, Microsoft implemented the Gateway Service for NetWare (GSNW) and included it in Windows NT Server.

The Gateway Service for NetWare is a Windows NT Server utility that allows Windows NT Server to act as a gateway to a NetWare network. With the Gateway Service for NetWare, customers can deploy Windows NT Server as a communication server and enable SMB clients to have access to the NetWare LAN. Suppose that a NetWare-based network administrator has an MS-DOS-based client that he has never been able to include in his NetWare network. With GSNW deployed on a Windows NT Server-based machine, he can now integrate this MS-DOS-based computer into the NetWare network, making for easier and less costly administration.

The Gateway Service for NetWare also allows NetWare customers to deploy the protocol of their choice on the desktop, while still retaining access to the NetWare LAN. Therefore, customers can choose to gradually deploy TCP/IP as their strategic protocol, while eliminating the costs associated with a rip-and-replace approach.

The Gateway Service for NetWare gives Microsoft SMB-based clients access to NetWare file and print resources via Windows NT Server. This is done by setting up a virtual drive or printer on the Windows NT Server-based computer which represents an actual NetWare partition or printer. The older Microsoft clients make SMB-based file and print service requests to these virtual devices on the Windows NT Server-based machine. These requests may be transported via the NetBEUI or TCP/IP transport protocols; these are the protocols typically used on these SMB-only clients.

The SMB-based requests are then reformatted into NCP-based requests by the Gateway Service for NetWare and sent via IPX/SPX to the NetWare server. NCP responses are sent back from the NetWare server to the Windows NT Server, reformatted into SMBs by GSNW, and sent to the client. To maintain NetWare security and license requirements, GSNW allows the administrator to restrict GSNW use to licensed NetWare users and limit the total number of concurrent gateway connections.

A further benefit is of the GSNW is remote access to a NetWare server. Windows NT Server RAS supports up to 256 concurrent. And, because GSNW resides on the Windows NT Server, NetWare users can also benefit from Windows NT Server's *Remote Access Service* (RAS), which allows remote users to dial into the Windows NT Server and, via the GSNW, access a NetWare server. Windows NT Server RAS is a sophisticated and versatile tool, giving transparent use of the network via a standard phoneline, an ISDN, or an X.25 connection.

The net result of the Gateway Service for NetWare is that Windows NT Server allows an administrator to add newer technology to the network at his own pace, without the cost and effort of replacing all of the older technology at once. It also allows NetWare clients to choose which protocol they want to use on the desktop without losing LAN connectivity. Flexibility and cost-containment: two goals of Microsoft's Services for NetWare.

Following is a view of an integrated Windows NT Server and NetWare network with GSNW deployed.

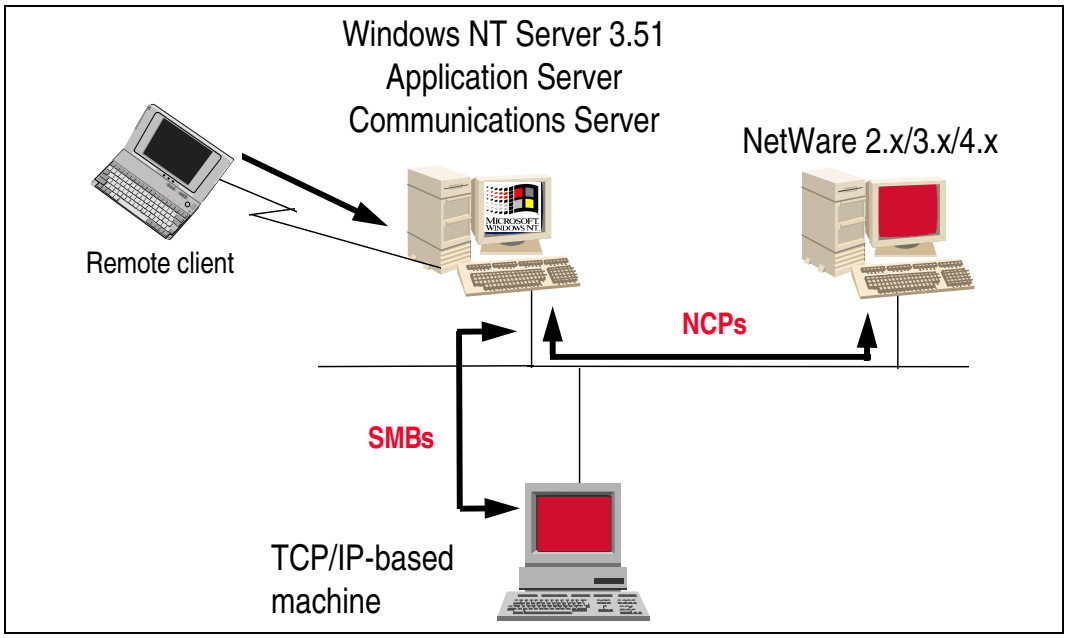

Figure 11: Gateway Service for NetWare

Centrally Managing Windows NT Server and NetWare

Microsoft recently announced the beta version of Microsoft Directory Service Manager for NetWare. Directory Service Manager for NetWare is a Windows NT Server utility that copies NetWare user and group account information to Windows NT Server and incrementally propagates any changes to the accounts back to the NetWare servers. All this is done without ever installing any software on the NetWare servers.

Directory Service Manager for NetWare was developed to solve a critical need in today's mixed network environment: the need for central management of NetWare 2.*x* and 3.*x* clients from a Windows NT Server-based machine during the transition to a Windows NT Server-based network. Windows NT Server has always been able to centrally manage Windows-based clients, with single logon to file and print services and all of Windows NT Server's applications. Now, Microsoft has also solved NetWare's problems of centralized management and single network logon with Directory Services Manager for NetWare. With DSMN, an administrator can centrally manage NetWare 2.*x*/3.*x* clients in a mixed Windows and NetWare environment, giving NetWare clients the same access as Windows clients to Windows NT Server's services and applications.

Having integrated Windows NT Server into the NetWare network, customers can minimize the cost of managing and using this mixed network. Directory Service Manager for NetWare is part of an overall Microsoft strategy to help NetWare customers:

- easily access the advanced networking services of Windows NT Server, such as Windows NT Server Directory Services
- integrate powerful, multi-purpose Windows NT Server-based machines into their existing NetWare network—Windows NT Server can supply both the file and print services NetWare customers use today, as well as advanced application, communication, and management services
- transition their NetWare network onto a single, easy-to-manage Windows NT Server foundation

With Directory Service Manager for NetWare, the mixed Windows NT Server and NetWare server network becomes easier to manage. Administrators only have to maintain one user account and associated password for each end-user on the network. End-users only need to remember one password and user account to get single logon access to file and print resources on the NetWare server, and file, print, and application resources on Windows NT Server.

Further, by taking advantage of the Windows NT Server Directory replication, end-users are assured that they will always have access to their network-based resources. For the administrator, Directory Service Manager for NetWare makes it easy to manage account information in a mixed network from a Windows NT Server-based machine.

Directory Service Manager for NetWare also supports a trial synchronization of the directory information on a NetWare server and the Security Accounts Manager (SAM) on a Windows NT Server. A trial synchronization allows the administrator to configure all the parameters of the synchronization and run it without actually transferring any information to the Windows NT Server-based machine. This gives the administrator the opportunity to catch any errors or problems with the synchronization, such as duplicate user accounts, before the actual synchronization. Also, the trial synchronization can be performed while the network is in use, meaning that no services need to be interrupted to try the DSMN synchronization. This advantage saves time and money, and ensures that there is no loss of productivity.

Following is a view of a Windows NT Server and NetWare integrated network with DSMN deployed.

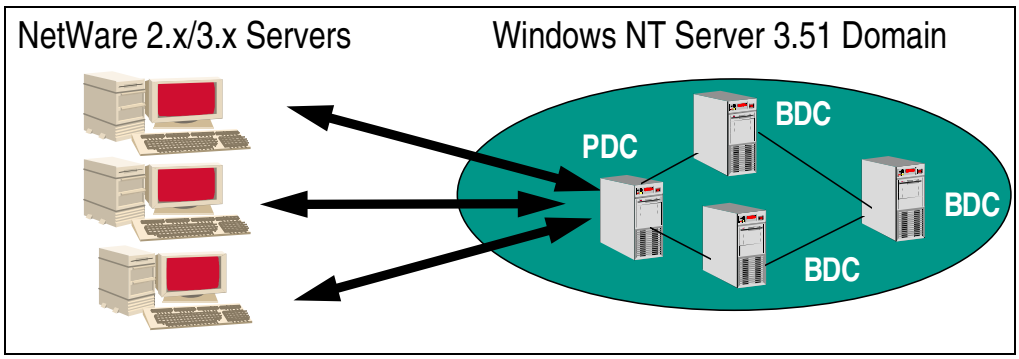

Figure 12: Directory Service Manager for NetWare

Migrating NetWare Servers to Windows NT Server

Windows NT Server integration into NetWare environments is further eased by the Migration Tool for NetWare. The Migration Tool for NetWare is a utility that automatically ports NetWare 2.*x* and 3.*x* user accounts, group accounts, security information, logon scripts, administrator accounts, files, directories, file attributes, and file rights to Windows NT Server. By automatically migrating these components, administrators can save the time, effort, and cost of recreating them manually while upgrading to Windows NT Server. In addition, it performs this migration without affecting the NetWare server in any way. As a result, NetWare user services are not interrupted.

The Migration Tool is extremely flexible. It allows administrators to migrate one or more NetWare servers to a single Windows NT Server-based machine. By consolidating multiple NetWare servers on a single, multi-purpose Windows NT Server-based computer, administrative overhead can be significantly reduced. Additionally, administrators can control which information is migrated, account restrictions, and administrative rights.

The Migration Tool also supports trial migrations of data and accounts. This is a critical tool for testing a migration before performing it. For example, multiple user accounts for the same user are common in NetWare environments since each NetWare server maintains a separate bindery. Since Windows NT Server-based networks require only one account per user, the Migration Tool highlights duplicates and provides options for dealing with them. The administrator can examine detailed logs of such errors, compensate for them, and rerun trial migrations until he is satisfied with the migration results. The actual migration can then be performed. The trial run is another aspect of Microsoft's recognition of the complexity of a mixed network environment and the need for exactitude in transferring any information. And, like the DSMN trial synchronization, the trial migration can be performed while the network is up and running, meaning that no network services are interrupted by the trial.

The Migration Tool operation requires the IPX/SPX transport protocol and the Gateway Service for NetWare to provide the communication path between the NetWare server(s) and the Windows NT

Server-based machine. File and Print Services for NetWare may also be used after the migration to ensure NetX and VLM client access to file and print services on the Windows NT Server-based computer.

Following is a view of an integrated Windows NT Server and NetWare network with the Migration Tool deployed.

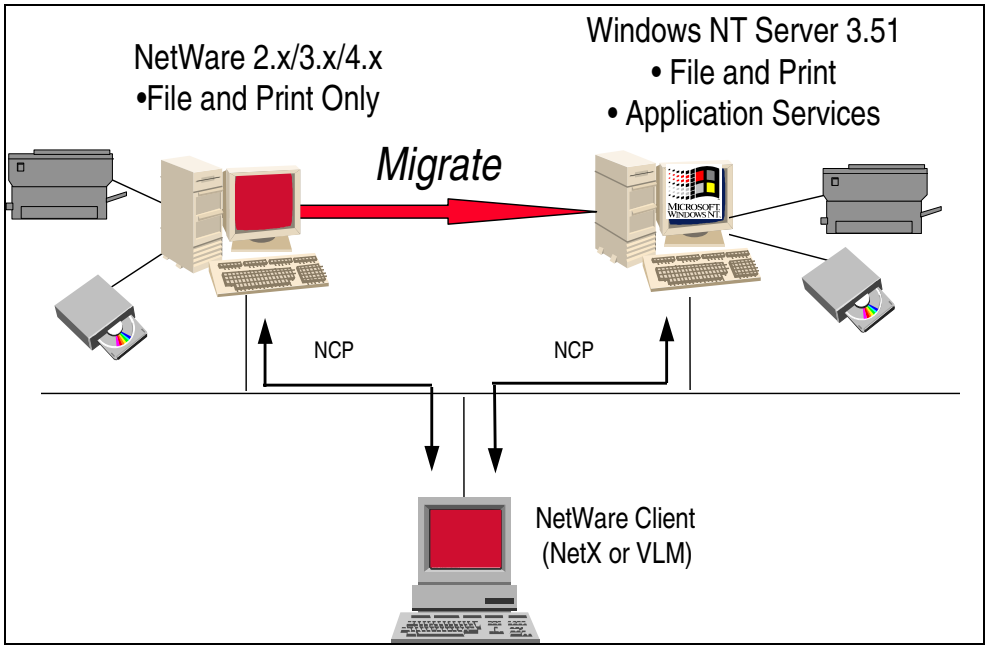

Figure 13: Migration Tool for NetWare

UNIX (TCP/IP) Integration

Like NetWare integration, Windows NT Server offers rich integration with TCP/IP-based UNIX environments. Windows NT Server supports the protocol (TCP/IP), application programming interfaces (APIs), utilities, and management protocols common in a UNIX environment. As a result, UNIX network users can easily integrate Windows NT Server-based computers and take advantage of Windows NT Server's advanced capabilities. In a UNIX network, Windows NT Server provides:

- file, print, and application services to both PC and non-PC clients
- support for Simple Network Management Protocol (SNMP) systems
- UNIX printer access for non-UNIX clients, such as PCs and Macintoshes
- automated IP address configuration and name resolution (described above in the "Managing TCP/IP" section of this document)

TCP/IP is comprehensively supported by Windows NT Server. All Windows NT Server-based services, including file, print, messaging, database, host connectivity, and systems management are available via TCP/IP. Any client that supports the SMB file and print service protocol can access Windows NT Server file and print services directly via TCP/IP. These clients include Windows for Workgroups, Windows NT Workstation, and Windows 95. Additionally, Windows NT Server supports the File Transfer Protocol (ftp) and Telnet utilities common in TCP/IP environments. Non-SMB clients such as UNIX workstations, Macintosh, and NetWare NetX-based machines can access Windows NT Server-based files using ftp or telnet. Third party support is also available for clients that use Network File Sharing (NFS) utilities.

Windows NT Server also ships with a Line Printer (LPR) utility so that UNIX clients can send print jobs to Windows NT Server-based printers. Similarly, PC and Macintosh clients can send print jobs to UNIX print servers and printers attached directly to the network via TCP/IP.

As with IPX/SPX, Windows NT Server-based applications can be accessed via TCP/IP and an interprocess communication protocol (IPC). Microsoft BackOffice server applications support

Named Pipes and Windows Sockets for interprocess communication over TCP/IP. Third party server applications provide similar IPC support.

Windows NT Server is also a full SNMP agent. As a result, it provides status information to common SNMP consoles such as Digital's PolyCenter or Hewlett-Packard's OpenView®. Information is provided upon any request from the console application.

Macintosh Connectivity

Windows NT Server also offers connectivity services for Macintosh networks with its *Services for Macintosh* (SFM). With SFM, Macintosh machines need only the Macintosh operating system software to operate as clients in a Windows NT Server network: no additional software is necessary. These services allow a Macintosh machine to fully access files and applications on a Windows NT Server-based machine, resulting in greater flexibility.

Services for Macintosh also allow the Macintosh to access printers on a Windows NT Server-based machine, just as it would a Postscript printer in an AppleTalk network, by routing the Macintosh through the Windows NT Server-based machine. This access is performed because SFM understand the AppleTalk transport protocol and can forward data from one Macintosh subnetwork to another. This routing capability also lets a PC can access a Postscript printer, just as it would any other printer in a Windows NT Server network.

Windows NT Server's ability to serve as an AppleTalk router means that a Macintosh network can migrate completely to a Windows NT Server-based network, without changing any of the software or hardware on the client side. Both the network administrator and the end-user benefit in terms of cost, ease of use, and familiarity.

Windows NT Server's SFM utilities allow Macintosh machines access the server just as a PC would. SFM contain an AppleTalk-compatible network transport protocol, a Win32® service that understands Apple's file service protocol, as well as a Win32 service that understands Apple's print service protocol. By providing these protocols, SFM give Macintosh machines complete file and print access to a Windows NT Server-based network, as well as use of Microsoft applications. They also give PCs complete access to an AppleTalk network.

OTHER KEY FEATURES

Remote Access Service Connectivity

Windows NT Server 3.5, as well as the newly released Windows NT Server 3.51, enables off-site users to connect to LAN-based resources via a standard phone line, an ISDN, or an X.25 connection. Microsoft *Remote Access Service* achieves this connectivity by supporting various clients, APIs, and protocols, and is included in Windows NT Server. The RAS Server takes remote client requests and rebroadcasts them over the LAN. The RAS client code is bundled with the following clients: Windows® 3.*x*, Windows for Workgroups, Windows NT Workstation, and will support Windows 95 when it ships (MS-DOS support is bundled with the Windows NT Server software).

Microsoft RAS also supports non-Microsoft clients by using third-party software. With RAS, a client can access Microsoft file and print resources, NetWare file and print resources, as well as LAN-based distributed applications.

In order for RAS to work, both the server and the client must use the same set of framing, transport, and file and print service protocols over the remote link. The *framing protocol* (such as PPP) establishes from the outset of the remote session such things as packet size, compression type, authentication of the remote user, and security. The *transport protocol* (such as NetBEUI or TCP/IP) performs the actual transmission of data between the server and the client. The *file and print service protocol* (such as SMB) requests file and print services. When a user does actually access the network using RAS, it will look like he is directly connected to the network. He can then participate fully in the network, accessing files, databases (such as SQL Server), and communicating with others via e-mail.

The transparency provided by RAS makes it extremely useful for telecommuters, traveling employees, as well as network administrators. With Windows NT Server 3.51, RAS supports up to 256 simultaneous sessions, meaning the server can handle more remote sessions than ever before. Also, RAS Compression is added, resulting in better and faster throughput, higher productivity for the user, and lower server stress.

Windows Clients and Windows NT Server: A Great Networking Combination

Windows 95 and Windows NT Workstation make great clients in a Windows NT Server-based network because they are designed, from the ground up, to exploit all of Windows NT Server's strengths. This means that they include utilities that make networking easier, more powerful, and more productive, for both the end-user and the administrator. There are several key features worth noting, including:

- **The new Windows 95 User Interface.** Designed from the ground up to be network enabled.
- **Integration.** Both Windows 95 and Windows NT Workstation are designed to integrate into any networking environment by providing the IPX/SPX, TCP/IP, and NetBEUI protocols.
- **DHCP awareness.** Both Windows 95 and Windows NT Workstation are DHCP-enabled, making TCP/IP networking much easier.
- **Remote Access Service.** Both Windows 95 and Windows NT Workstation are excellent remote clients, taking full advantage of Windows NT Server's Remote Access Service.
- **Common API set.** Both operating systems share Windows NT Server's development API, Win32.
- **Long file names.** Both operating systems support Windows NT Server's long file name capabilities, meaning that file names are not altered when files are stored on either the desktop or the server.

The new Windows 95 User Interface, for instance, is more than simply a new look to the Windows operating system. The new UI is designed around the networking features of Windows 95, making it easier for the end-user to network. For example, suppose Jim Smith needs to know the names of all the shared computers in his workgroup. With the new UI, all he has to do is click on the button labeled "Network Neighborhood" and he is given a view of those machines and their names (see the following graphic). Other new tools, such as the Windows 95 Explorer, are explicitly designed to make networking with Windows NT Server and Windows clients easy and powerful.

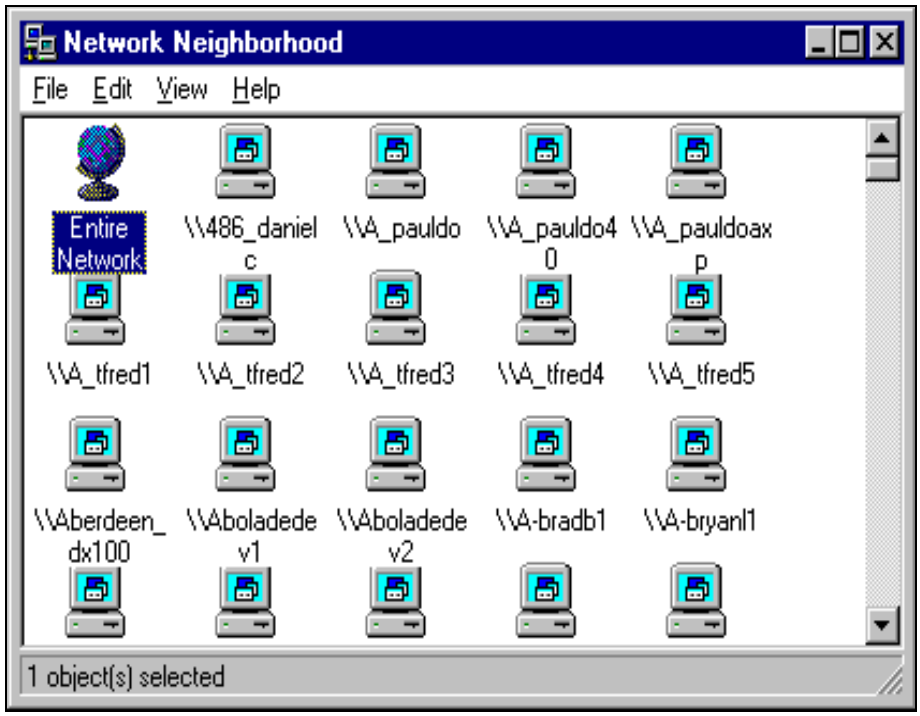

Figure 14: Windows 95 Explorer

The new Windows 95 User Interface is the networking environment of tomorrow's Windows NT Server and Workstation, which will incorporate the new UI. Windows NT's modular architecture means that, as new technology is developed, Windows NT Workstation and Server can accommodate changes without redesigning the operating system. The new Windows 95 UI is an example of this: the new UI will be incorporated into Windows NT Server and Windows NT Workstation in the near future. The new UI on Windows NT is part of Microsoft's commitment to consistency and tight integration between Windows clients and Windows NT Server.

Microsoft's networking philosophy is to let our clients work with any server and to enable our server to work with any client. This means that client systems running MS-DOS or Windows NT Workstation, for example, should be able to access servers based on Windows NT Server, Novell NetWare, UNIX, and mainframes. Similarly, Windows NT Server will work with MS-DOS, OS/2®, UNIX, Windows, Windows NT Workstation, NetWare, and Macintosh-based clients.

Windows 95 and Windows NT Workstation can integrate into most networks, but this does not mean that every network, be it a UNIX, Macintosh, or NetWare-based network, can take full advantage of these clients and their built-in networking capabilities. While both desktop operating systems make excellent clients in any network, they were designed to take full advantage of everything a Windows NT Server-based network has to offer. A Novell NetWare-based network, for example, can not take advantage of the DHCP awareness of Windows 95 (or Windows NT Workstation) because NetWare does not support DHCP. Windows NT Server does. Similarly, Novell's clients in a Windows NT Server-based network can do everything they can do in a NetWare-based network. But Microsoft's clients in a Windows NT Server-based network can do even more.

Suppose, for example, that Jim Smith wants to go the New York office. Prior to DHCP, Jim would have had to call his administrator in Los Angeles and get a TCP/IP address, type it in (hoping not to make an error) and, every time he moved the machine to another location, perform the task over again. Not only is this time consuming and troublesome for Jim, it is also a heavy burden on the network administrator, who has to be available any time Jim, or anyone else, wants to boot a computer.

Now, Jim can take his DHCP-enabled, Windows 95 or Windows NT Workstation-based computer with him, and DHCP will automatically assign him a TCP/IP address, so he can take full advantage of his network just as if he were at his desk. The combination of Windows

NT Workstation and Windows NT Server makes the network administrator's job less costly and easier because he does not have to manually assign a TCP/IP address to Jim whenever Jim boots his machine. Separately, each operating system is designed to integrate with a wide variety of server and client systems. Together, they deliver a complete networking architecture that exploits the combined power of Microsoft's desktop and server operating systems.

Similarly, both Windows 95 and Windows NT Workstation support Windows NT Server's Remote Access Service (RAS). Suppose that Jim Smith leaves New York and goes to Atlanta, where his company does not have an office. By using RAS, Jim can dial into his office, using a standard phone line, ISDN, or X.25 connection, and it will look to him just as if he were in his office. He can then do everything that he would typically do in his office because every application, utility, and file is available to him. Because Windows NT Server does multi-protocol routing, Jim's computer can use any protocol and still utilize Windows NT Server's RAS. Also, with RAS Compression, Jim has better and faster throughput, higher productivity, and lower server stress. The administrator also benefits from Windows NT Server's RAS because less time is spent on supporting remote users and more is spent on creating a more productive networking environment.

Windows clients and Windows NT Server also share a common development platform: the Win32 set of API's and OLE. Since they share the same APIs as Windows NT Server, they can take advantage of the already established and large independent software vendors' (ISV) applications support that Windows currently enjoys. ISVs, for their part, can leverage their knowledge of the Win32/OLE APIs to build powerful applications more easily. This guarantees the availability of great solutions that meet customer's needs, both today and in the future.

Windows 95 and Windows NT Workstation both support long file names, which means that the 8.3 character file name is no longer necessary. Both, like Windows NT Server, support file names up to 256 characters. This means that these clients can display the more intelligible long file names supported on Windows NT Server.

For example, a file name that would be displayed as "win95exa.doc" on a NetWare client can now be displayed as "Windows 95 Examples of the New Interface" on a Windows 95 or Windows NT Workstation client, a much more descriptive and intelligible name. File sharing is a lot easier when everyone knows what each file is. The end-user spends less time opening and closing documents to see what they are and more time being productive.

Windows 95 and Windows NT Workstation make great networking clients for all of the following reasons:

- **Easy Installation and Management.** Install Windows 95 over the network with a single boot floppy using Windows NT Server's exclusive Network Client Administrator.

  Also, eliminate the need to manually track TCP/IP addresses with Windows NT Server's DHCP and WINS capabilities. Now it is easy to give TCP/IP access to all of the systems on your network, even portables, because Windows NT Server automatically assigns TCP/IP addresses.

  Lastly, merge the power of a WAN with the LAN's ease of use by using Microsoft's TCP/IP software, included at no extra charge in Windows 95, Windows NT Workstation, and Windows NT Server. Windows NT Server is the only network operating system that lets Windows 95-based clients access files directly over TCP/IP.

- **Long file names.** Windows NT Server's 32-bit file system supports the same long file names as Windows 95 and Windows NT Workstation. This means that file names are not altered when you store files on the server. For older 16-bit applications that require MS-DOS style "8.3" file names, Windows NT Server automatically generates 8.3 names using the same format as Windows 95 and Windows NT Workstation.

  The combination of the Windows client and Windows NT Server delivers a single logon to the desktop and the server. Users type in their password once and are automatically logged into both their desktop and all servers at the same time. Both Windows 95 and Windows NT Workstation work with Windows NT Server's directory service without any additional software.

- **Remote Access Service.** Windows NT Server includes remote access service that is 100% compatible with Windows 95 Dial-in networking or Windows NT Workstation remote access service. Remote access service works with any Windows 95 or Windows NT Workstation protocol and supports internal routing. This means that Windows NT Server can be the dial-in gateway to any network, including the Internet and NetWare.
- **The robust platform for today's, and tomorrow's, network.** Windows NT Server's modular architecture means that, as new technology is developed, Windows NT Server can accommodate changes without redesigning the operating system. The new Windows 95 UI is an example of this, as the new UI will be incorporated into Windows NT Server and Windows NT Workstation in the near future, without requiring re-engineering or re-deployment of existing applications.

To take advantage of all of these features, install Windows NT Server and one of the new breed of Windows clients. Windows 95 and Windows NT Workstation are excellent clients in a Windows NT Server-based network because they were designed to exploit all of Windows NT Server's strengths, making management of the network easier and less costly. While each integrates very well in any network, no NetWare, IBM, or Macintosh-based network can support all of their features. By integrating Windows NT Server into any one of these networks, you can begin to take advantage of its tremendous power and versatility, and migrate the entire network at your own pace without interrupting user services.

A Windows NT Server-based network with Windows 95 or Windows NT Workstation as the client fulfills all of the requirements for a successful distributed system. All of the benefits for the end-user and administrator point to the same goals: superior service to customers and better, more informed decisions through fast, useful access to information. Windows NT Server and Windows clients are the right combination to help you attain these goals.

OTHER NETWORK OPERATING SYSTEM STRATEGIES

As discussed, Microsoft believes that one of the largest impediments to strategic computing is that most vendors network operating systems are not designed to enable effective information access. A careful evaluation of competitive network operating systems, such as Novell NetWare confirms this perspective. Below are the seven primary requirements for effective networking, according to Novell. Each of these requirements is being provided by its NetWare products, according to Novell. [2]

1. Directory service
2. Integrated messaging
3. Multiprotocol routing
4. Network management
5. Security
6. File
7. Print

While these are indeed important technologies, Novell makes it clear that it does not yet address the specific needs of today's networking customer. To clarify, it seems appropriate to make a more direct comparison between Windows NT Server and Novell NetWare and to determine what, precisely, are the customer needs in a network operating system. It is important to note that Windows NT Server and NetWare are different network operating systems. However, the customer's needs are consistent, regardless of the operating system they choose. To review, Microsoft's customers have indicated that they need:

- A reliable, multi-purpose network foundation that supports basic networking services (such as high-performance file and printer sharing) and the robustness, security, scalability, and widely-used development environments (i.e., Win32 and OLE) necessary to support a new generation of mission-critical, client-server business applications.

[2] Novell Corporation, "When you Purchase Your Network, Make Sure You Get ALL the Pieces" 1994

- A network foundation that is easy for administrators to install and manage while providing the desktop integration necessary to make it easy for end users to use.
- A system that integrates seamlessly with the network systems customers have today including NetWare, UNIX, IBM SNA, PATHWORKS, Banyan® VINES®, and Apple® Macintosh.
- An operating system architecture that allows for easy integration of new technology without requiring complete system re-engineering. Windows NT Server's modular, microkernel design was implemented specifically for this purpose.

It is possible that Novell understands these requirements as well since they have indicated they will be developing a new "SuperNOS" specifically to meet these needs. Of course, Microsoft offers much of this functionality today with Windows NT Server. We have invested over 6 years and $600 million in the development of Windows NT Server and continue to invest at a vigorous pace. Microsoft currently dedicates over 3000 employees to the design, development, testing, and support of Windows NT Server and we plan to continue with this level of commitment.

Microsoft's investments have yielded a robust, secure, high-performance platform with a common development interface, strong support from the developer community, thousands of available applications, and tight integration with today's most commonly used desktop operating systems. In addition, Windows NT Server integrates easily with the network operating systems that customers use today while providing a foundation upon which customers can easily build new technology. Having spent the time and money to build the foundation, Microsoft continues to work vigorously to improve the usability, manageability, interoperability, and performance of this foundation.

Novell still faces many of the challenges Microsoft has already met. NetWare 4.1 is a dramatic improvement over previous versions of NetWare largely due to the implementation of NetWare Directory Services (NDS). NDS solves a long-standing problem for NetWare 2.*x* and 3.*x* users—it offers them a single logon to the network and centralized administration of all servers. And the NDS management interface (the "tree"), while not perfect, is quite elegant. Novell's challenge lies in the fact that NDS is an interface on top of NetWare's existing file and print operating system technology. As a result, Novell must build the secure, robust foundation necessary to support mission-critical business applications. At the same time, they must compel application developers to build solutions on their platform. These are major challenges that are, arguably, even greater than those met by NDS. For customers, this means deploying NetWare 4.1 today will solve existing problems with NetWare 2.*x* and 3.*x* but it will not provide the long term foundation they need.

Microsoft has already built both the foundation and the development community. With Windows NT Server, customers can build solutions that integrate their organizational information systems and deliver critical business information to the people who need it most. With these solutions, organizations can make better, more informed business decisions and provide truly superior service to their customers. Microsoft has also solved NetWare's problems of centralized management and single network logon with Directory Services Manager for NetWare. And with File and Print Services for NetWare, NetWare customers can gain the full benefits of Windows NT Server-based applications and file and print services without changing their existing NetWare client software. Therefore, it is easier for customers to gain the benefits of both the Windows NT Server foundation and NDS by deploying Windows NT Server. And Microsoft is committed to making the foundation even better.

The following table is a detailed feature comparison chart designed to help customers understand the differences between Windows NT Server 3.51, NetWare 3.12, and NetWare 4.1.

Server Product Comparison

The following pages provide a detailed comparative listing of features between the Windows NT Server and NetWare operating systems. This comparison is based on information published by Novell on the current implementations of their products. The key to the individual line item is:

✓Functionality of the feature is included within the product (unless otherwise noted)

When appropriate, additional information is provided in the table or in footnotes.

SUMMARY OF KEY FEATURES

	Windows NT Server	*NetWare 3.12*	*NetWare 4.1*
Architecture:			
Pre-emptive multitasking	✓		
Processors – Intel	✓	✓	✓
Processors – RISC	MIPS, DEC Alpha AXP, PowerPC		
Symmetric multiprocessing	✓32 Processors		
Virtual memory	✓		
Microkernel architecture	✓		
Memory protection for apps and subsystems	✓		(for debugging only)
Transports:			
	NetBEUI, IPX, TCP/IP (native)		IPX, TCP/IP (tunneling)
File System:			
Efficient subblock allocation	✓ 512 bytes	✓ 16K	✓ 16K
File compression	✓		✓
High performance Asynchronous I/O	✓		
Performance optimizations:			
Dynamic cache	✓ 1GB per process		(static cache)
Security:			
Designed to meet C2 Security	Orange Book – Evaluated Products List Red Book ✓		Red Book – Vendor Assistance Phase Orange Book – N/A
Single logon compatibility for client-server applications	✓		✓
Centralized security event auditing	✓		
Network Management:			
GUI utilities	✓		✓
Remote administration, performance and event monitoring	✓		
DHCP support for TCP/IP	✓		
WINS support for TCP/IP	✓		
Performance monitoring:			
Graphical remote performance monitoring	✓		
Fault tolerance:			
File System Recovery Log	✓		

DETAILED FEATURE COMPARISON

	Windows NT Server	*NetWare 3.12*	*NetWare 4.1*
Architecture:			
Multi-user operating system	✓	✓	✓
Pre-emptive multitasking	✓		
Processors – Intel	✓	✓	✓
Processors – RISC	MIPS, DEC Alpha AXP, PowerPC		
Symmetric multiprocessing	✓up to 32 Processors		
Asymmetric multiprocessing		✓	
Clustering			
Minimum memory RAM	16 MB	4 MB	6 MB
Maximum memory RAM	4 GB	4 GB	4 GB
Paged virtual memory	✓		
Dynamic memory cache	✓		
Maximum number of user connections	unlimited	250	1000
32-bit operating system	✓	✓	✓
Dynamic loading of services	✓	✓	✓
Memory protection of applications	✓		
Audit alerts	✓	✓Audit Y, Alerts N	✓
Structured exception handling	✓		
Microkernel based architecture	✓		
Protected subsystems	✓		
Hardware abstraction layer	✓		
Unicode support	✓		
Installable File systems	✓	✓	✓
NIC support - Client:			
16-bit Ethernet support	✓	✓	✓
32-bit Ethernet support	✓	✓	✓
16-bit Token Ring support	✓	✓	✓
32-bit Token Ring support	✓	✓	✓
NDIS support	✓		✓
ODI support	✓	✓	✓
Third party driver support	✓	✓	✓
NIC support - Server:			
16-bit Ethernet support	✓	✓	✓
32-bit Ethernet support	✓	✓	✓
16-bit Token Ring support	✓	✓	✓
32-bit Token Ring support	✓	✓	✓
NDIS support	✓		
ODI support	✓ Novell requestor only	✓	✓
Third party driver support	✓	✓	✓
Multiple network adapters	✓	✓	✓
Other hardware support:			
CD-ROM	✓	✓	✓
SCSI adapters	✓	✓	✓
Plotters	✓	✓	✓
Scanners	✓		

	Windows NT Server	*NetWare 3.12*	*NetWare 4.1*
Transports:			
IPX	✓	✓	✓
IPX Dial-in	✓	✓	✓
Packet Burst	✓	✓	✓
LIP	✓	✓	✓
AppleTalk	✓	✓ (extra cost)	✓ (extra cost)
NetBEUI	✓		
TCP/IP (tunneling)		✓ (extra cost)	✓ (for 500 users, SRP is $24,990)
TCP/IP (native)	✓		
OSI	✓ (in Win32 SDK)	✓	
DECNet	✓ (DEC)		
DLC	✓	✓	✓
Internal routing	✓RAS only	✓	✓
IPCs:			
Named Pipes (client side)	✓	✓	✓
Named Pipes (server side)	✓		
Sockets	✓	✓	✓
Transport Library Interface	✓		
DCE compatible RPC	✓		
LU 6.2, LU1, LU0, LU2, LU3	✓ (SNA Server)	✓(NetWare SAA)	✓(NetWare SAA)
HLLAPI	✓ (3rd party)	✓ (3rd party)	✓ (3rd party)
Local Procedure Call (LPC)	✓		
Semaphores	✓		✓
Mutexes	✓		✓
Timers	✓		
Asynchronous Procedure Calls	✓		
File System:			
Maximum number of file locks	unlimited	100K	100K
Maximum number of file opens	unlimited	100K	100K
Maximum file size	17 billion GB	4 GB	4 GB
Efficient subblock allocation	✓ 512 bytes	✓	✓ 16K
File compression	✓		✓
Transaction-based file system	✓		✓
Support for DOS files	✓	✓	✓
Support for Mac files	✓	✓	✓
Support for OS/2 files	✓	✓	✓
Support for NFS	✓ 3rd party	✓extra cost	✓extra cost
Volumes/files span drives	✓	✓	✓
Total disk storage	408 million TB	32 TB	32 TB
Maximum volumes/server	25	64	64
Maximum physical drives/server	limit of hardware	1024	1024
Maximum partition size	17,000 TB	drive size	drive size
Maximum volume size	17,000 TB	32 TB	32 TB
Disk quotas	✓ 3rd party	✓	✓
High performance asynchronous I/O	✓		
Memory mapped File I/O	✓		
Maximum length of file name	255	255	255
Long file names made visible to MS-DOS programs	✓	✓ only on HPFS	✓ only on HPFS

	Windows NT Server	*NetWare 3.12*	*NetWare 4.1*
Performance optimizations:			
Dynamic cache	✓ 1GB per process		(static cache)
Elevator seeking	✓	✓	✓
Read-ahead caching	✓	✓	✓
Background writes	✓	✓	✓
Overlapped seeks	✓	✓	✓
Split seeks	✓	✓	✓
Directory hashing	✓	✓	✓
Directory caching	✓	✓	✓
File caching	✓	✓	✓
Virtual Memory	✓		
Returnable memory	✓	✓	✓
Data scattering		✓	✓
Security:			
Designed to meet C2 security	✓ Redbook ✓ Orangebook		✓ Redbook Orangebook N/A
Designed to meet B2 security	✓ 3rd party		
Single login to network	✓		✓
Single, secure logon	✓	✓	✓
Single logon for compatible client/server apps			
Minimum password length restriction	✓	✓	✓
Passwords encrypted	✓	✓	✓
Packet signing (secure authentication)	✓	✓	✓
Password aging	✓	✓	✓
Password history	✓	✓	✓
Min. time until password can be changed	✓	✓	✓
Account lockout	✓	✓	✓
Restrict login to specific workstation	✓	✓	✓
Replaceable client login	✓		✓
Limit concurrent connections for single user		✓	✓
Restrict login by time and day	✓	✓	✓
Set account expiration date	✓	✓	✓
Disconnect when access time expires	✓	✓	✓
Re-key password verify	✓	✓	✓
Configurable administrative rights	✓	✓	✓
Centralized security event auditing	✓		
Security event alerts	✓		
File system auditing	✓	✓	✓
Directory and File rights:			
Read	✓	✓	✓
Write	✓	✓	✓
Execute	✓	✓	✓
Delete	✓	✓	✓
Change permissions (Grant)	✓	✓	✓
Take ownership	✓	✓	✓
List Directory	✓	✓	✓
Create files in Directory	✓	✓	✓

	Windows NT Server	*NetWare 3.12*	*NetWare 4.1*
User rights:			
Access workstation from network	✓		
Logon locally	✓		
Back up files and directories	✓	✓	✓
Restore files and directories	✓	✓	✓
Change the system time	✓		
Shut down system locally	✓	✓rconsole	✓rconsole
Force system shutdown remotely	✓	✓rconsole	✓rconsole
Load and unload device drivers	✓	✓rconsole	✓rconsole
Manage audit and security logs	✓		
Take ownership of files or other objects	✓	✓yes, with supervisor rights	✓yes, with supervisor rights
Security auditing:			
Audit user security transactions	✓	✓	✓
Audit user file transactions	✓	✓	✓
Audit administrator transactions	✓	✓	✓
Audit file-creation statistics	✓	✓	✓
Audit volume statistics	✓	✓	✓
Filter audit logs	✓	✓	✓
Audit security policy changes	✓		
Audit restart or shutdown of system	✓		✓
Non-dedicated server	✓		with OS/2 add-in product
Printing:			
Remote printer port on Workstation	✓	✓	✓
Peer print services	✓		
Assign priorities to print queue	✓	✓	✓
Multiple queues to a single printer	✓	✓	✓
Multiple queues on multiple printers	✓	✓	✓
Multiple printers on one queue	✓	✓	✓
Postscript supported	✓	✓	✓
Maximum shared printers per server	unlimited	16	255
Cross platform printing (OS/2)	✓	✓	✓
Cross platform printing (UNIX)	✓	✓extra cost	✓extra cost
Cross platform printing (NetWare)	✓	✓	✓
Cross platform printing (SNA)	✓	✓	✓
Remote queue management	✓	✓	✓
Support for multiple forms		✓	✓
Network attached printer support	✓	✓	✓
User notification of job completion	✓	✓	✓
Operator notification of print problem	✓	✓	✓
Printer alerts:			
Out of paper	✓	✓	✓
Print request deleted	✓	✓	✓
Print request completed	✓	✓	✓
Printer off-line	✓	✓	✓
Paper jam	✓	✓	✓
Needs specific form		✓	✓
Configure error reporting to specific users		✓	✓

	Windows NT Server	*NetWare 3.12*	*NetWare 4.1*
Network Management:			
Command line utilities	✓	✓	✓
GUI utilities	✓		✓
Remote administration, performance, and event monitoring	✓	✓	✓
Asynch remote administration	✓	✓	✓
Remote installation	✓	✓	✓
Remote upgrade	✓	✓	✓
Remote corrective service	✓	✓	✓
Remote session security	✓	✓	✓
Remote modem callback	✓	✓extra cost	✓extra cost
DHCP support for TCP/IP	✓		
WINS support for TCP/IP	✓		
Performance monitoring:			
View total percent CPU use	✓	✓	✓
View total privileged CPU use	✓		
View total user CPU use	✓		
View logical disk use	✓	✓	✓
View physical disk use	✓	✓	✓
View cache utilization	✓	✓	✓
View packets/bytes sent	✓	✓	✓
View page/faults per second	✓		
View number of active processes	✓	✓	✓
View number of active threads	✓		
View processor time by process	✓		
View processor time by thread	✓		
Log performance statistics	✓		
Delegating admin responsibility:			
Account operators	✓	✓	✓
Backup operators	✓	✓	✓
Directory administrator	✓	✓	✓
Enterprise administrator	✓	✓	✓
Print operator	✓	✓	✓
Replication operator	✓		
Server operator	✓	✓	✓
Alert messages:			
Volume is getting full	✓	✓	✓
Volume is full	✓	✓	✓
Error log is full	✓	✓	✓
Connection slots depleted	✓	✓	✓
Memory for resource allocation depleted	low virtual memory alert	✓	✓
Disk utilization above threshold	✓	✓	✓
Fault tolerance:			
File system recovery log	✓		
Redundant directory structures	✓	✓	✓
Directory verification during power-up	✓	✓	✓
Read-after-write verification	✓	✓	✓
Hot fix	✓	✓	✓

	Windows NT Server	*NetWare 3.12*	*NetWare 4.1*
Fault tolerance (cont.):			
Salvage/undelete	✓ (FAT only)	✓	✓
UPS support	✓	✓	✓
Disk duplexing	✓	✓	✓
Disk mirroring	✓	✓	✓
Software RAID 5	✓		
Server mirroring	✓3rd party	✓	
Dynamic volume sets	✓		
Backup:			
Backup/restore of server disk w/security	✓	✓	✓
On-line backup of account files	✓	✓	
Backup utility included	✓		
Workstation backup (Windows for Workgroups, Windows NT Workstation)	✓	✓ TSR	✓ TSR
Automatic file replication service	✓		
Server Job Scheduling	✓		

0895 Part No. 098-61666