Microsoft Windows 2000 Server

Operating System

Comparing Sun Solaris 7, Windows NT Server 4.0, and Windows 2000 Server

White Paper

Abstract

This paper compares Windows® 2000 Server, Windows NT® Server, and Sun Solaris 7. It focuses on key issues IT managers should consider when comparing these network operating systems.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

03/00

Executive summary

The choice of a network operating system is a strategic, long-term decision driven by the demands that organizations have for a platform on which to build business solutions. Although networking, data services and print sharing are still vital requirements, organizations today are relying on the server operating system to provide many additional services such as:

- Running business applications and providing an infrastructure for the next generation of distributed applications.
- Running Internet and intranet sites.
- Providing a comprehensive communications infrastructure to provide services such as remote access through VPN and dial-up connections.
- Providing comprehensive directory and desktop management services.

As opposed to hiring and training administrators to manage multiple server operating systems, customers are moving to multipurpose server operating systems to reduce their Total Cost of Ownership (TCO). Therefore, throughout this technical comparison, three operating systems, Microsoft® Windows® 2000 Server, Windows NT® Server 4.0, and Sun Microsystems' Solaris 7, will be evaluated based on their ability to provide a solid integrated infrastructure for data services, print sharing, directory services, system management, and distributed application services for the enterprise customer. The configuration for Solaris 7 considered the latest software bundles, including Easy Access Server 3.0 and Enterprise Server 1.0.

Overview of Windows 2000 Server

Windows 2000 Server has been designed from the ground up as an integrated multipurpose operating system. Three versions of Windows 2000 Server will be available this year:

- **Windows 2000 Server**
- **Windows 2000 Advanced Server**
- **Windows 2000 Datacenter Server**

For the latest information on the features in each version of Windows 2000, customers should visit the Web site: http://www.microsoft.com/windows2000.

Windows 2000 Server, like Windows NT Server, is a 32-bit operating system. Windows 2000 Server will support the Intel IA-64 chip architecture and a 64-bit version is planned for release later this year. The 64-bit version will extend the physical and virtual memory capabilities of Windows 2000 Server as shown in the following table.

Table 1. Comparing 64-Bit and 32-Bit Windows 2000

Component	**64-Bit Windows 2000**	**32-Bit Windows 2000**
Virtual Memory	16 TB	4 GB
Paging file size	512 TB	16 TB
Paged pool	128 GB	470 MB
Non-paged pool	128 GB	256 MB
System cache	1 TB	1 GB

Key technologies supported by Windows 2000 Server include:

- ❑ **File and Print Sharing** – The file and print sharing features in Windows 2000 Server provide customers with an advanced solution, offering a distributed file system, Internet printing, content indexing, dynamic volume management, and Plug-and-Play support.

- ❑ **Networking and Communications** – Networking infrastructure is complete and manageable – it offers true dynamic configuration, integrated dial-up and virtual private networking (VPN) with support for the latest Internet Engineering Task Force (IETF) VPN protocol suite, telephony and a quality of service (QoS) solution to guarantee bandwidth and network availability.

- ❑ **Application Services** – Windows 2000 Server provides customers with a scalable solution in terms of CPU and memory support. The combination of Clustering Services, component load balancing, and the Windows Load Balancing Service provides a comprehensive solution to increase scalability and reliability. Terminal Services provide a thin-client solution. And in Windows 2000, distributed file system (DFS) support has been added to Terminal Services.

- ❑ **Internet Services** – The Windows 2000 Internet services also offer a complete solution. Windows 2000 Server includes unrivaled Internet services for management, publishing, streaming media, and performance enhancement.

- ❑ **Management Services** – The Active Directory™ service in Windows 2000 Server is built completely around Internet-standards and offers extensibility and scalability. This makes it a solution on which to build enterprise-level directory-enabled applications. Microsoft Management Console (MMC) provides customers with a single, customizable interface for managing networking services and applications. The combination of IntelliMirror™ management technologies, Windows Installer, and Group Policy Services easily provides a comprehensive solution for software distribution and desktop management. For security, Windows 2000 Server supports Kerberos V5, smart card authentication, fully integrated public key infrastructure, and encrypted file system (EFS) services. Windows Management Infrastructure (WMI) is the Microsoft implementation of the Common Information Model (CIM), a public standard supported by the Desktop Management Task Force (DMTF). The WMI technology enables management applications to produce reports of network inventory, display system information, respond to events, start or stop system services, and send an eject command to a disk drive with replaceable media.

Overview of Windows NT Server 4.0

Windows NT Server is built on a 32-bit architecture and is available in three editions:

- ❑ **Windows NT Server** – The standard version of Windows NT Server is designed to handle workgroup needs and supports 4 GB RAM.

- ❑ **Windows NT Terminal Server Edition** – The Terminal Server Edition of Windows NT is designed for thin clients.

- ❑ **Windows NT Server Enterprise Edition** – The Enterprise Edition supports load balancing with up to 32 servers and 2-node clustering. It also supports up to 32 CPUs (through OEMs) and 4 GB RAM.

Windows NT Server provides many of the same services found in Windows 2000 Server; however, it lacks an extensible, hierarchical directory. Although the directory in Windows NT Server 4.0 provides organizations with a centralized directory for managing users and groups and single logon services, it is not as advanced as either Active Directory services or Sun Directory Services.

- **File and Print Sharing** – File and print sharing support in Windows NT Server is robust, although not as advanced as the file and print features in Windows 2000 Server.

- **Networking and Communications** – Basic protocol support is identical in Windows NT Server 4.0 and Windows 2000 Server. However, Windows NT Server 4.0 does not support Windows 2000 TCP/IP performance enhancements and requires a reboot for certain configuration changes. In remote access and VPN services, Windows NT Server 4.0 offers more features than Solaris 7 – including VPN services, additional protocol support, remote authentication dial-in user service (RADIUS) client support, additional password encryption options, and restartable file copy.

- **Application Services** – Application support in Windows NT Server 4.0 is outstanding, providing numerous capabilities such as message queuing, clustering and load balancing, and a thin-client solution in the Terminal Server Edition. Native distributed component support is also superior – the combination of COM and Transaction Server offers many capabilities not found in Solaris 7. Furthermore, with the addition of Active Server Pages (ASP), the power of COM-based applications can be extended to the Web.

- **Internet Services** – The Internet services in Windows NT Server 4.0 are comparable to Solaris 7, offering load balancing, content management, and protocol support including Simple Mail Transfer Protocol (SMTP) and Network News Transfer Protocol (NNTP).

- **Management Services** – Management services in Windows NT Server provide easy to use graphical tools, MMC management for key services, and the Zero Administration Kit to control desktops. However, the directory-based software distribution and Group Policy capabilities found in Windows 2000 Server do not have equivalents in Windows NT Server 4.0.

Overview of Solaris 7

Sun Solaris 7 is the first version of Sun Solaris to fully support a 64-bit architecture. Previous versions of Sun Solaris, named with the 2.X convention, partially supported 64-bit technologies. The 64-bit architecture gives Sun Solaris extended precision, large file support and large virtual address space support. Solaris 7 supports the Intel 64-bit chip architecture but current 32-bit Intel chips don’t take advantage of 64-bit enhancements. Sun Solaris has two server software extensions:

- **Easy Access Server** -- Easy Access Server is designed to provide an integrated bundle of services to users and administrators. Easy Access Server has extensions that make it possible to interoperate with Windows NT and to emulate Windows NT services. These services are authentication, file, and print. Domain services are referred to by Sun as directory services but do not emulate Active Directory or other directory services. Instead this feature allows Easy Access Server to emulate a Windows NT Primary Domain Controller (PDC). Solaris Easy Access Server also supports 64 CPUs and 64GB of maximum addressable memory.

- **Enterprise Server** -- Enterprise Server provides load balancing and 4-node clustering capabilities. The products that implement these features are Sun Cluster for clustering, Solaris Resource Manager for load balancing, and Solaris Bandwidth Manager for IP traffic management. Enterprise Server also supports 64 CPUs and 64GB of maximum addressable memory.

The focus of this white paper is on Solaris 7 with Easy Access Server 3.0 and Solaris 7 with Enterprise Server version 1.0. Enterprise Server provides high availability, reliability, and scalability features. These products are best compared to Windows NT Server 4.0 and Windows NT Server 4.0 Enterprise edition.

A key difference between Windows 2000 and Solaris 7 with the server extensions is pricing. When compared to the nominal cost difference between Windows 2000 Server, Windows 2000 Advanced Server and Windows

2000 Datacenter Server, the cost difference between Solaris Easy Access Server and Solaris Enterprise Server is quite significant. Solaris Enterprise Server is also considerably more expensive than Windows 2000 versions that support load balancing and clustering, namely Windows 2000 Advanced Server and Windows 2000 Datacenter Server.

As the white paper will show, Solaris server products make only a cursory attempt at providing customers with an integrated administration solution. The limited solutions that are available require considerable Unix expertise. Most of the services are simply provided as add-ons and lack common management interfaces. The Solaris product documentation makes it quite clear that the server extension products are simply add-ons of applications that run on top of Sun Solaris.

- ❑ **File and Print Sharing** – File and print services in Solaris 7 are extremely robust, with excellent native TCP/IP printing implementation. File sharing via the included TotalNET Server package for Windows, NetWare and Macintosh clients provides a strong framework for network file sharing. Solstice NFS clients are provided for integrating Windows 95, Windows 98 and Windows NT. Solstice NFS is provided as a separate software package, which is installed on Windows-based systems.

- ❑ **Networking and Communications** – Sun advertises that the Internet runs on Sun operating systems. Their excellent native TCP/IP support is the standard by which other implementations are judged. While support for Sun supplied hardware is excellent, users of the Intel version of Solaris 7 will find support for only a small subset of the available networking hardware. Routing and remote access services are available, but the native implementation of standard features, such as PPP, is very difficult to configure and lacks broad support for modem hardware. Solaris includes no telephony solutions but does offer a strong VPN solution through SunScreen SKIP.

- ❑ **Application Services** – Solaris 7 provides services to develop Java applications. However it does not provide message queuing services, a CORBA Object Request Broker (ORB), or comprehensive distributed component functionality, such as integrated transactions. This lack of application services makes Solaris a relatively limited choice.

- ❑ **Internet Services** – The Internet services in Solaris 7 provide organizations with full-featured HTTP and FTP services required to host Internet and intranet sites. It provides a strong development environment built around servlets and the JAVA IDL. However, it lacks true operating system integration. It also lacks support for many key features and standard protocols found in the Microsoft products. It does offer support for the Microsoft FrontPage® server extensions for SPARC.

- ❑ **Management Services** – Although it boasts an impressive feature-set, Solaris 7 lacks any sort of comprehensive management tool. Each individual application has its own tool with little or no commonality of behavior or interface. Many of the tools require their own separate logon process even when launched from the same session. The Solaris Management Console 1.0 is little more than a container that allows the various disparate management tools to be launched from the same place. While previous versions of Solaris did not support single logon or enterprise-wide authentication, both Easy Access Server 3.0 and Enterprise Server 1.0, support these features.

Introduction

Given the recent increase in corporate interest in the various UNIX and UNIX-derivative operating systems now on the market, and significant marketing on the part of Sun Microsystems for the Solaris 7 operating system, customers are asking how Windows NT Server 4.0 and Windows 2000 Server compare. This document examines the issues facing customers who wish to plan deployment of an enterprise network operating system. This document will compare the features of these operating systems in the following categories:

- **File and Print Sharing.**
- **Networking and Communications.**
- **Applications Servers.**
- **Internet/Intranet Servers.**
- **Management and Directory Infrastructure.**

Each deployment scenario will be covered in detail in this document. To make it easier for you to find information, each section uses one or more of the following subsections:

- **Section Summary** –The goal of this section is to provide you with high-level understanding of the key differences in Windows NT, Windows 2000 and Sun Solaris 7.
- **Feature Table** –This table provides an easy and efficient way to understand key differences in Windows NT, Windows 2000 and Sun Solaris 7.
- **Implementation Details** – There will be a Solaris 7, Windows NT Server 4.0, and Windows 2000 Server Implementation Details section for each category.
- **Solution Details** –Breaks down each solution and describes how it meets the fundamental customer requirements. This is where the most detailed information about each operating system can be found.
- **Comparison Summary** –Describes the differences between the three operating systems in a specific technology or solution.

File and Print Sharing services

Section Summary

File and print sharing services are important aspects of a network operating system. File and print sharing services implementations include the following:

- **File System.**
- **Storage services.**
- **Printer sharing services.**

In terms of feature-completeness, Windows 2000 Server offers more than the other two products. Its unmatched capabilities include a distributed file system (DFS), content indexing, dynamic volume management, a true hierarchical storage management services implementation, Web printing, Plug-and-Play printing, and advanced fault tolerance through Clustering Services.

Compared with Solaris 7, Windows NT Server 4.0 easily matches Sun's offering in some areas while falling short in others. However, Windows NT Server 4.0 comes out ahead of Solaris 7 because its file and printer sharing services are considerably less complicated. Windows NT Server 4.0 features a single architecture for both file and printer sharing and semi-standardized GUI-based management tools. Solaris 7 has multiple architectures for both file and printer sharing services and a mixed bag of command-line and graphical administration applications. Windows NT 4.0 is easier to administer and run on a daily basis, making it a better choice for the customer than Solaris 7.

The file system management implementation of Solaris 7 has more standards support than Windows NT Server 4.0, but does not support critical functions such as undelete which are standard on Windows NT Server. In EAS 3.0, the Solaris Data Backup Utility has been dropped from the server. This change means that you must acquire a backup solution separately from the server.

Solaris 7 also presents significant usability problems when it comes to managing volumes and file sharing. The tools in Solaris 7 lack integration, which makes finding the appropriate tool difficult. A combination of GUI-based administrative tools and command line actions are necessary to fully manage and configure storage and file sharing. Compared with Windows 2000 Server, Solaris 7 offers a similar level of features and functionality, but Solaris 7's lack of integrated management tools becomes a more glaring defect.

In the printing arena, Solaris 7 surpasses the features and functionality in Windows NT Server 4.0 and comes close to matching the capabilities in Windows 2000 Server. Previous versions of Solaris 7 lacked a powerful management tool. But Solaris 7 now comes with Solaris Print Manager 1.0, which allows you to install, view and manage printers anywhere on the network.

Feature Table

Feature	Solaris 7	Windows NT Server 4.0	Windows 2000 Server
File Sharing and Storage Services Features		NTFS	NTFS5
Integrated Namespace Support	■	■	■
File Compression	□	■	■
Block Sub-Allocation/Adjustable Block Size	■	■	■
Salvage/Undelete	□	■	■
Spanning	■	■	■
Mirroring	■	■	■
3-Way Mirroring	■	□	□
Duplexing	■	■	■
Striping without Parity	■	■	■
Striping with Parity	■	■	■
HSM/RSM APIs	■	□	■
Integrated Backup Software	□	■	■
Native Property Sets	□	□	■
Sparse File Support	□	□	■
Volume Change Log	□	□	■
Junction Points / Mount Points	■	□	■
Distributed Link Tracking	□	□	■
Disk Quota Support	■	□	■
Self-describing Disks	□	□	■
Online Disk Management	■	□	■
Removable Storage Management	■	□	■
Hierarchical Storage Management	■	□	■
Disk Defragmentation Support	□	□	■
I_2O Support	■	□	■
Fiber Channel Support	■	□	■
IEEE 1394	■	□	■
Distributed File System	■	□	■
Integrated Load Balancing	■	□	■
Integrated Replication	□	□	■
Integrated Site Proximity	□	□	■
Integrated Fault Tolerance	■	□	■
Printer Sharing Services Features			
Directory Services Integration	■	□	■

TCP/IP (LPD) Printing Support	■	■	■
Internet Printing	■	□	■
Print Server Clustering	■	□	■
Image Color Management 2.0 API	■	□	■
Plug-and-Play Printing	□	□	■
Automatic Configuration	□	□	■
Supports TCP/IP Print Servers	■	■	■
Supports NetWare (IPX/SPX Print Servers)	■	□	□
Supports DLC Print Servers	□	■	■

(Black boxes indicate features included in the operating system.)

File Sharing and Storage Services

At the physical level, file sharing services should include integrated namespace support, file compression, configurable block size, mirroring, duplexing, striping with or without parity, removable device support, link tracking, and a means to automatically archive unused data while allowing it to remain available to the user. In terms of providing additional services, a good file system implementation provides integrated content indexing, user-definable file properties, and a tracking log to audit storage services usage.

From a management perspective, volume defragmentation, backup and restore, easy security administration tools, disk quotas, and the ability to configure file systems dynamically without downtime are also key features. Finally, support for the latest performance-enhancing hardware technologies is important in high usage environments.

Solaris 7 Implementation Details

Solaris 7 offers a comprehensive, but at times complex, file sharing service implementation. Out of the box, Solaris 7 provides support for two file systems – UNIX File System (UFS) and the industry standard Network File System (NFS).

In terms of value added file system features, Solaris 7 provides the following on the UFS and NFS file systems:

- **Block Sub-Allocation** allows the operating system to use unused space within each physical block to store additional information, resulting in less wasted disk space – especially on systems with large block size.
- **Self-describing Disks** allow for metadata that describes disk configuration to be stored on the device itself and to be replicated. Self-identification of managed disks ensures that disk controller ownership transfers are completely error free. Disk reconfigurations and cluster disk ownership transfers are also error-free.
- **Data Striping** at the software level. With this, a volume can be equally spread between two or more physical devices, greatly enhancing read performance and reducing disk device wear.
- **Mount Points** are tools provided in UFS for grafting storage name spaces together. It allows the mounting of a file system at the directory level on an existing volume – similar to junction points in Windows 2000. Mount points are transparent to applications unless an application is explicitly instructed to notice them. This means that users can use junction points to reroute applications or users accessing a local UFS directory to any other partition.
- **Disk Mirroring** allows disks to be physically replicated to other disks, block-for-block, within a server. In the event of a failure, the mirror will automatically activate, allowing the server to continue operations despite having lost a physical disk. Solaris 7 supports 2-drive and 3-drive mirror sets.

- **Data Migration** provides the necessary operating system hooks at the file system level to allow a Hierarchical Storage Management (HSM) implementation. With HSM, infrequently used data can be archived to removable storage such as tape, CD-ROM, or optical disk but still readily available to users. In the event a user requests an archived file, it will be automatically loaded and retrieved.

Network File Sharing

The Network File System (NFS) is a standard for network file sharing and provides support for any client with NFS software. Solaris 7 includes the Solstice NFS Client 3.2, which provides integrated client access for Windows 95, Windows 98, and Windows NT. Management of network shares is best accomplished from the command line, with no straightforward GUI tool available to create and maintain network shares.

Sun provides an enhanced version of NFS that is designed specifically for sharing files over the Web. This version, called WebNFS, extends the standard features of NFS to the Web and enables Web-based collaboration. With WebNFS, users can access data on the Web just as they access local data. WebNFS uses HTTP over TCP/IP to communicate and is designed to be more reliable and dynamic than FTP. Many Windows-based applications have similar functionality built-in. For example, with Office 2000 applications, you can access Web folders directly in the Open File dialog box. In both Windows NT and Windows 2000, you can also grant access to data over the Web through Web sharing, which is similar to file sharing. For true Web-based file handling, Windows users can rely on World Wide Web Distributed Authoring and Versioning (WebDAV), which is discussed later in this white paper.

Removable Storage Support

CD-ROM support is provided natively in Solaris 7. Support for other removable media (other than backup media) is fairly limited and becomes problematic if the media is not SCSI-connected.

Volume Management

As mentioned earlier, the DiskSuite 4.2 tool included in Solaris 7 is probably the best management tool in the package. From this tool, detailed control is available over the hard drives installed in the system and the manner in which data is laid out on the drives. Data Striping, data striping with parity, mirror sets, and other storage fault tolerance features are controlled from this same interface.

File system backup and restore tools are provided by the Solaris Data Backup Utility. This is a licensed version of the Legato Networker enterprise backup tool. Unlike the backup utilities included with Windows NT 4.0 and Windows 2000, the Solaris Data Backup Utility is a full featured, fully functional enterprise backup tool that supports cross-platform clients other than UNIX. However, Sun decided to package Solaris Data Backup Utility separately from Solaris 7. This means you must acquire and install this product.

Storage Hardware Enhancements

Lastly, Solaris 7 also provides support for the I_2O standard on the Intel platform. With I_2O, CPU overhead associated with disk requests can be offloaded to intelligent microprocessors on I_2O-compliant systems and disk controllers, lowering server CPU usage and improving performance.

Windows NT Server 4.0 Implementation Details

Windows NT Server 4.0 provides support for two file systems as part of the operating system: FAT16 and NTFS. For the purpose of this review, only NTFS will be evaluated as the FAT16 support has been provided merely for compatibility with prior versions of Windows. First introduced with Windows NT version 3.1, NTFS is Microsoft’s 64-bit, next-generation file system.

Name space support in NTFS is integrated into the file system. Hence, files of virtually any type can be created and saved on NTFS-based systems.

NTFS, as it exists in Windows NT Server 4.0, features many advanced storage features including the following:

- **Compression** allows for the compressed storage of files and directories so that less physical space is required, reducing the amount of disk space actually utilized. Compression is configurable on a volume, directory, or file basis.
- **Spanning** is available, allowing administrators to extend volumes across multiple physical disks.
- **Data Striping** implements RAID Level 0 functionality at the software level. With this, a volume can be equally spread between two or more physical devices, greatly enhancing read performance and reducing disk device wear.
- **Data Striping with Parity** implements RAID Level 5 functionality at the software level. With this, a volume can be spread between three or more physical disks with parity information distributed across all disks. In the event of a single disk device failure, the parity information can be used to keep the volume and system running until the system administrator can rectify the problem, greatly reducing the chance of disk-related server failure.
- **Data Mirroring/Duplexing** allows for the physical duplication of disk devices in real-time, providing for instantaneous recovery in the event of a failure. With mirroring, you use one disk controller for both mirrored drives. With duplexing, you use two disk controllers, one for each mirror drive, which prevents a controller-related problem from causing a system crash.

Disk Quotas

Windows NT Server 4.0 provides no disk quota support, although the functionality is available from third-party independent software vendors (ISVs). As would be expected, full security is available for the restriction of access to files and directories. For Windows NT-based systems running in a workgroup, the local account database will be used. For servers participating in a domain environment, the domain’s account database will be used. The Windows Explorer utility provides a means to administer security using friendly extensions to Windows Explorer for managing access control.

Network File Sharing

Any NetBIOS-capable clients capable of connecting to Server Message Block (SMB) shares can connect to and access files from NTFS shares. Additionally, with the optional Services for NetWare and Services for UNIX add-ons, file shares can be made accessible to NCP-compatible NetWare clients and any UNIX system that supports the NFS protocol.

Volume Management

No removable storage or Hierarchical Storage Management features are present in Windows NT Server 4.0. Management of volumes is through the graphical Disk Administrator utility and the command-line CHKDSK is used for volume repair. Changes are not dynamic and require the server to be rebooted.

Finally, backup and restore support is provided through the Windows NT Backup Utility. Windows NT Backup provides a rudimentary feature set to backup and restore files and directories on any Windows NT-compatible ATAPI or SCSI tape device. Registry information, domain controller configuration, and file systems are all supported as targets for backup and restore by Windows NT Backup.

Windows 2000 Server Implementation Details

Windows 2000 Server features the latest implementation of the NTFS file system. It provides numerous additional features and enhancements over the prior versions of NTFS. Additionally, support for the FAT16 file system is carried over from Windows NT Server 4.0 and support for the FAT32 file system found in Windows 98 has been added. Again, for the purpose of this document, Windows 2000 Server shall be evaluated only on the NTFS file system.

The NTFS implementation in Windows 2000 Server contains all of the features found in the Windows NT Server 4.0 NTFS implementation and also offers the following improvements to the core file system:

- **Native Property Sets** are now supported on any file or directory. These are indexed periodically by the integrated Indexing Services, providing for fast searches based on properties such as document author. Potential applications include flat file annotation, metadata caching, and content management.
- **Sparse File Support** allows an application to create huge files without actually committing disk space for every byte. For example, a user can create a 42-GB file that only has data written to the first and last 64K segments within the file. In this case, the file would only physically occupy 128K of space on the disk, but in all other respects it would act as if it were 42-GB in size. Sparse file support provides for many interesting applications such as sparse arrays and circular queues.
- **Reliable Change Journal** tracks all changes to files and directories over long periods of time and across system reboots. With this feature, I/O can be analyzed and the creation, renaming, and deletion of files can be easily tracked. Potential applications include I/O performance analysis and application state recovery.
- **Mount Points** are tools provided in NTFS for grafting storage name spaces together. Essentially, it allows the mounting of a file system at the directory level on an existing volume – similar to mount points in UNIX. Mount points are transparent to applications unless the application is explicitly instructed to notice them. You can reroute applications or users accessing a local NTFS directory to any other partition. Local file systems mounted on top of mount points can be accessed through them even if they do not have drive letters assigned – essentially removing the 26 drive letter limit.
- **Distributed Link Tracking** provides a service to preserve shortcut integrity when users move or rename files. With this feature, client applications are allowed to track link sources that have been moved. Links can either be shortcuts for files or embedded OLE objects, such as a Microsoft Excel worksheet embedded in a Word document. Changes tracked include renaming the link source, moving the link source within the same volume, moving the link source between two volumes on the same computer, moving the link source between two computers in the same domain, moving a volume from one computer to another in the same domain, renaming a computer within a domain, changing a network share under which the link source is shared, or any combination of these scenarios.

Disk Quotas

Windows 2000 Server now provides full disk quota support. Quotas are tracked on a per-user, per-volume basis and users are charged only for files they own. Events are automatically logged when users exceed warning thresholds and quota limits. Policies are configurable to set up wide-scale remote management of disk quotas. Quota information can be saved along with other volume information during backup. Restoring a backup will always override quota limits, provided that the user performing the operation has the appropriate backup privileges. Windows 2000 also provides scripting extensions that you can use to build powerful quota reporting tools.

Bulk Access Control List (ACL) Checking

Also added to Windows 2000 Server is the Bulk ACL Checking feature. With it, administrators can perform accessibility tests against multiple files by specifying an arbitrary access mask. This allows administrators to perform such tasks as:

- Determining what user *X* can do with *N* files.
- Check multiple ACLs simultaneously for file access.

File System Content Indexing

Full content indexing capabilities have been added to Windows 2000 Server with the introduction of integrated Index Services. This completely indexes all files available on a file system according to content or attributes. Index Services is fully integrated with Windows Explorer. It can be used from the Find Files or Folders dialog.

Index Services can also be used to index content on the Internet or remote sites. The index can then be queried via Web-based forms. All operations of Index Services are automatic, including updates, index creation and optimization, and crash recovery. Manageability of Index Services is extremely powerful. It can be configured to operate on a per file or per directory basis. It takes full advantage of other enhancements to NTFS and also features full integration with the Windows 2000 Hierarchical Storage Management (HSM) feature, providing for the indexing of content archived through HSM.

Volume Management

A complete, dynamic volume management has been provided in Windows 2000 Server in the Disk Management tool. Authored by VERITAS Software Corporation, the Disk Management tool provides the following functionality:

- **Online Disk Management** support has been added, allowing administrators to perform all common disk administrative tasks without having to shut down the system. A volume can be created, extended, or mirrored without requiring a reboot.
- **Self-describing Disks** allows for metadata that describes disk configuration to be stored on the disk itself and then be replicated. Self-identification of managed disks ensures that disk controller and other disk reconfigurations or cluster disk ownership transfers are completely error-free.
- **Simplified tasks** represent one of the most important features of the new Disk Management tool, which is based in the Microsoft Management Console. Consequently, the Disk Management MMC snap-in tool is considerably easier to use than the Disk Administrator tool it replaces. It provides shortcut menus to walk customers through tasks that can be performed on a selected object. Wizards guide users through creating partitions and volumes and initializing or upgrading disks.

Hierarchical Storage Management (HSM)

Windows 2000 Server provides a complete Hierarchical Storage Management (HSM) solution with the inclusion of Remote Storage Services (RSS) – a data archiving solution based on technology provided by Seagate Technology, Inc. RSS makes it easy for customers to increase disk space on a server without adding additional disk capacity. RSS automatically monitors the amount of space available on the local hard disk. When the free space on a managed primary hard disk drops below a preset threshold, RSS will automatically remove local data that has been copied to remote storage devices, while still keeping the directory and property information active. Since removable optical disks and tape are less expensive on a cost per megabyte basis than hard disks, this represents an economical way to provide both maximum storage and optimal local performance.

RSS uses an administrator-defined rule set to move infrequently accessed files to long-term storage. Reparse points are used to store information about the file in the file system. This information itself is physically stored in a stub file containing the reparse point whose data points to the device where the actual file is now archived. Windows 2000 can use this information to retrieve the file in the event a user submits a request for it.

Removable Storage Management

Windows 2000 Server provides a comprehensive removable storage solution in the form of the Removable Storage Manager (RSM). With RSM, management tasks such as mounting and dismounting media are now performed automatically. RSM presents a common interface to robotic media changers and media libraries. It enables multiple applications to share local libraries and tape or disk drives and controls removable media within a single system.

Seagate Software has provided an update to the Windows NT Backup software as the backup and restore solution for Windows 2000 Server. It is based entirely on RSM technologies and sports a new user interface. It has wizards to ease common backup and restore tasks. Windows NT Backup in Windows 2000 Server represents a significant step forward over the version in Windows NT Server 4.0. Most importantly, Windows NT Backup now supports a variety of optical and magnetic storage devices not supported in Windows NT Server 4.0. The Windows NT Backup in Windows 2000 Server can backup and restore all file systems, the registry, and its Active Directory service.

Disk Defragmentation

Disk defragmentation support has been added to Windows 2000 Server based on technologies from Executive Software. This reorganizes clusters on a disk volume so that files, directories, and free space are more contiguous. Depending on the extent of fragmentation, overall system performance can be improved dramatically. The defragmentation utility is implemented as a Microsoft Management Console (MMC) snap-in. It can defragment FAT, FAT32, or NTFS file systems.

Network File Sharing

File sharing client support remains essentially the same as that in Windows NT Server 4.0. NetBIOS clients running over TCP/IP, IPX/SPX, and NetBEUI are supported by default. NetWare-compatible (NCP) and UNIX (NFS) clients are supported with optional add-ons.

Storage Hardware Enhancements

Storage hardware support also has been enhanced in Windows 2000 Server to provide support for the following new, storage technologies:

- **Fiber Channel** is a technology for 1-gigabit-per-second data transfer that maps common transport protocols such as SCSI and IP. It is an open standard, defined by ANSI and OSI, which operates over copper and fiber-optic cabling at distances of up to 10 kilometers. Fiber Channel storage support is implemented under Windows 2000 Server by layering into the SCSI stack.

- **IEEE 1394** is a standard for high-speed peripheral interconnects. The most compelling attributes of IEEE 1394 are simple connectivity combined with bandwidth for multimedia. The benefits include a single-connection for A/V data and control.

- **I_2O** is fully supported in Windows 2000. Consequently, performance can be enhanced on machines utilizing I_2O-capable storage cards as processing can be offloaded to the storage card’s microprocessor rather than burdening the server’s CPU.

Distributed File System

The most significant enhancement to file services in Windows 2000 Server is the addition of the Distributed File System (DFS). The DFS provides a single name space for disparate file system resources at the enterprise level. So, using a single name, users can access network resources spread out over many different servers within an organization.

Technically DFS is organized as a logical structure, called a tree, which is totally independent of the physical resources. Logical volumes can be added to a DFS tree and are made available to end-users. Logical volumes can be directories on disk, entire Windows NT volumes, or another DFS tree, allowing for sub-trees.

Security is fully integrated with Windows 2000 Server. Administrators can impose access restrictions based on users, groups, and quotas. Permissions are physically associated with the shared resources themselves and are not propagated as part of the DFS tree structure.

DFS tree structure is published to Active Directory, which serves as a central coordinator for all of the topologies for all DFS trees. DFS configuration information is automatically replicated to all DFS trees within the Active Directory service. Consequently, in the event of a server failure, the topology and all resources that were not physically stored on the failed system remain available throughout the outage and configuration is restored properly when the failed system returns to online status.

Resources also can be replicated via DFS. By creating alternate, replicated resources and assigning them to a DFS root or volume, administrators can ensure that users have absolute, uninterrupted access to their files. Synchronization is totally automatic and does not require administrator intervention once configured. In addition to providing fault tolerance, replication also serves to enhance performance by balancing load between servers and by reducing network traffic via redirection so that users only connect to the server that is physically closest to them over their LAN/WAN.

Consequently, in comparison to standard file sharing services, DFS provides many additional benefits that directly benefit the customer including the following:

- **Fault Tolerance** - When multiple servers are used as the basis for a DFS share, users will be automatically redirected to available servers. Consequently, if one of three systems is unavailable, users are transparently redirected to the remaining online servers, providing better availability and reliability than non-DFS file sharing solutions. Additionally, all configuration information is replicated in Active Directory so that it is available across all domain controllers on the network.

- **Load Balancing** – When multiple servers are used to host a DFS share, load is automatically balanced between available servers. The benefit to customers is enhanced performance and better availability under high usage scenarios.

- **File Replication –** A DFS share can also be made up of multiple shares across multiple services with automatically replicated file content. Synchronization is totally automated and requires no user intervention. With file replication, absolute availability is guaranteed. If any one of the servers within DFS fails, users will be able to continue working and be transparently redirected to one of the other online replicas without any interruptions in service.

- **Site Proximity –** DFS automatically redirects users to the DFS share that is physically closest to them. This process is completely transparent and provides for greatly reduced network utilization by keeping users working locally (assuming a share is available) rather than having to access information over a wide area link.

File Sharing and Storage Services Summary

Windows 2000 Server and the NTFS file system represent the best solution for the enterprise customer. At the physical level, NTFS supports junction points, sparse files, distributed link tracking, and a volume change log. Windows 2000 Server also provides complete content indexing of the file system, hierarchical storage management. A major new feature in Windows 2000 Server is dynamic volume management. This allows for live configuration changes without requiring a server reboot. Windows 2000 Server also provides a powerful and full-featured suite of tools for backup, restore, and disaster recovery. It also supports all three of the latest developments in next-generation storage technologies – I_2O, IEEE 1394, and Fiber Channel. Finally, Windows 2000 Server Distributed File System (DFS) provides for integrated load balancing, fault tolerance, and replication services – features that are unmatched by either Solaris 7 or Windows NT Server 4.0.

In terms of functionality, the Windows NT Server 4.0 implementation falls behind that of Windows 2000 Server and Solaris 7. When compared with Windows 2000 Server, Windows NT Server 4.0 falls short by not offering Fiber Channel, IEEE 1394, I_2O, dynamic volume management, hierarchical storage management, removable storage management, disk quotas, junction points, sparse files, distributed link tracking, complete content indexing, and a volume change log. As Solaris 7 almost matches the feature set of Windows 2000 in this regard (though lacking such features as built-in file compression and disk defragmentation support), it provides a superior environment to Windows NT 4.0. The DiskSuite 4.2 tool used to manage and configure drive configuration and utilization is one of the few complete tools in Solaris 7 that provides a high level of integrated usability in terms of management and configuration. Unfortunately, however, DiskSuite is no longer bundled with the server. Also, although IEEE support is provided on the Solaris for Intel platform, there are no actual 1394 devices supported at this time.

Printer Sharing Services

In conjunction with file sharing services, printer sharing represents one of the most fundamental aspects of a network operating system. For the purpose of this document, each network operating system shall be evaluated on its ability to share local printers, support hardware-based print server devices, and interoperate with the TCP/IP Line Printer Daemon (LPD) standard for IP-based printing. Additional areas evaluated are client support, printer device support, and management tool support.

Solaris 7 Implementation Details

In Solaris 7, the Print Manager component of Solstice AdminSuite has been implemented as a separate product. The new Java-based version, called Print Manager 1.0, can run from any Solaris or Windows NT-based desktop and allows system administrators to perform all essential printer management functions. Using Print Manager 1.0, you can install printers locally or remotely, configure printer settings, modify printer access controls and delete printers as well.

Still, the configuration and installation process is more complex than in either Windows NT or Windows 2000. Each system with a printer attached gets both the SunSoft Print Client and SunSoft Print Server software installed. There is a limited number of printers supported with the emphasis on printers that can use PostScript. All of Solaris printing is LPD-based and there is no equivalent to the simple “attach a printer and install its driver” experience that a user can get with any current version of Windows. There is no Plug and Play printer support. Each printer attached to a standalone server or installed as a network printer requires the same convoluted installation process. The Windows NT 4.0 installation process of attaching the printer locally and electing to share it on the network is far more straightforward than the convoluted process to provide a network shared printer in Solaris 7.

Network printers can be found through the Solaris naming service (NIS or NIS+) once the SunSoft Print Client software has been installed. And since the NIS service (but not NIS+) can integrate with the Sun Directory Service, printers are made available to users of the directory service. While this makes finding network printers considerably easier than in Windows NT 4.0, this aspect of the Solaris network printing implementation lags behind the simplicity in Windows 2000.

Windows NT Server 4.0 Implementation Details

Windows NT Server 4.0 features a complete network printer sharing architecture. Unlike Solaris 7, a single unified architecture makes planning, configuration, deployment, and ongoing administration easier.

Windows NT Server 4.0 contains printer drivers for all popular printers, making device installation and configuration an easy task. Sharing support is provided for all parallel and serial printers by default. Hardware print server devices are supported via the DLC protocol for Digital Network Parts, Lexmark DLC Network Ports, HP JetDirect network ports, and via TCP/IP for Lexmark TCP/IP Network Port-compliant devices. Additionally, because Windows NT Server 4.0 uses a modular device architecture, additional device support and print server support can easily be added from the thousands of drivers available from third party OEMs.

Printer sharing services are provided to all NetBIOS-capable clients over the NetBEUI, TCP/IP, and IPX/SPX network protocols. Additionally, LPD-capable clients running the TCP/IP protocol can also connect and print via Windows NT Server 4.0, as full LPD server support is provided. Management is accomplished through the GUI interface present in the Printers folder, which is stored in the Windows Control Panel. As would be expected, printing rights can be fully restricted and auditing is supported as part of the Windows NT Server 4.0 security model.

Beyond basic printer sharing support, Windows NT Server 4.0 features the automatic download and configuration of device drivers, greatly easing a client's task when using shared printing resources. Additionally, printer pooling provides a single share point for client connectivity that can be load-balanced between multiple printers.

Windows 2000 Server Implementation Details

Windows 2000 Server improves on the printing support found in Windows NT Server 4.0 by adding the features summarized below:

- **Internet Printing** provides a full printer management solution over the Web. Users can print to a URL at local or remote sites. Potential applications include such things as commercial printing, hotel business centers, and Internet faxing. Additionally, print queue status can be viewed from any browser, allowing users and administrators alike to monitor status over the Internet or an intranet. Finally, print drivers can be downloaded and installed over the Internet automatically as part of the Windows 2000 printing implementation. For example, if a user wants to print to a neighbor's printer over the Internet, the driver can be downloaded and automatically installed on the user's computer directly from the neighbor's machine assuming security criteria have been met.

- **Active Directory Integration** allows users to easily share and locate printers across the network. Using a standard printer object that is stored in Active Directory, users can search for printers on the network by attributes such as location and capabilities.

- **Print Server Clustering** allows organizations using Clustering Services to provide transparent failover of printer sharing services to ensure absolute availability.

- **Image Color Management 2.0 API** provides the ability to send high quality color documents to a printer or to another computer faster, easier, and with greater consistency.

- **UniDrive5** offers improved color printing, support for OEM customization (allowing application developers to exploit printing device features without custom development) and an overall increase in printing speed.

- **Support for Plug and Play** makes the installation and setup of printers for the workstation more straightforward. Users no longer need to know about driver models, printer languages, or ports – printers are automatically discovered and configured.

- **Enhanced Management Tools** allow for quick-and-easy setup of printing on common network configurations. This allows administrators to get up and running faster, and to more easily set system-wide printer defaults.

Printer Sharing Services Summary

Windows 2000 Server boasts a complete feature-set, a powerful architecture, and easy management. Its networked printing services implementation is equivalent or superior to Microsoft Windows NT Server 4.0 in every area. . Additionally, Windows 2000 Server features fault-tolerant printing services, Web-integration and management, and industry-standard Plug-and-Play support.

While Solaris 7 does offer a GUI-based tool for managing and installing printers and software as well as the ability to integrate printers into a naming service, the installation and configuration of the print server and print client software is very complex.

Although Windows NT Server 4.0 does not feature the directory integration available in Solaris 7, its architecture and management are considerably simpler and less complicated, making it a more readily deployable solution. Additionally, it is the only solution besides Windows 2000 Server to offer support for DLC-based print server.

Networking and Communications

Section Summary

The networking and communications infrastructure is the most fundamental aspect of a network operating system. It provides connectivity and interoperability with client systems as well as other server-based operating systems. This infrastructure includes network architecture (physical device and media support), protocol support, networking services, Routing and Remote Access Services, and virtual private networking (VPN) services, Wide Area Network (WAN) connectivity, telephony, and Quality of Service (QoS). The best network operating system is that which offers the best balance of feature depth and ease of management in the above-mentioned areas.

Of the three network operating systems, the Windows 2000 Server network and communications infrastructure provides the most feature-complete and highly usable solution. Windows 2000 Server is highly available, as configuration changes are totally dynamic in most cases and do not require server downtime, and it is the only network operating system to offer a QoS implementation.

Windows NT Server 4.0 features telephony, and a VPN solution but does not, offer a QoS implementation. Manageability is entirely GUI-based but cannot compare with the ease-of-use, consistency, and additional capabilities featured in the Windows 2000 Server MMC, and configuration changes almost always require a server reboot.

Solaris 7 does not offer telephony solutions of any kind but does offer a strong VPN solution through SunScreen SKIP. Manageability is complex, as almost every aspect of configuration requires the use of a combination of command line tools and GUI-based tools. In general, availability is better than Windows NT Server 4.0, as fewer reboots are required for configuration changes.

Feature Table

Feature	Solaris 7	Windows NT Server 4.0	Windows 2000 Server
Network Architecture			
Ethernet	■	■	■
Fast Ethernet	■	■	■
Gigabit Ethernet	■	■	■
Token Ring	■	■	■
ARCnet	□	■	■
FDDI	■	■	■
Native ATM Support	■	□	■
Auto-Detects Devices at Install	■	■	■
Auto-Detects Devices Post-Installation	□	□	■
Configure Hardware as Part of OS	■	□	■
Configuration Changes Require Reboot	□	■	□
Supports NIC Hot-Swap	■	□	□
Supports Plug and Play	□	□	■
Power Management Support	■	□	■

Protocol Support			
TCP/IP	■	■	■
IPX/SPX	■	■	■
NetBEUI	■	■	■
DLC	□	■	■
AppleTalk	■	■	■
Supports Previous Clients on TCP/IP	■	■	■
Supports Previous Clients on IPX/SPX	□	■	■
Allows Selective Adapter/Protocol Bindings	■	■	■
Allows Protocol Binding Order Adjustment	□	■	■
Allows Selective Service/Protocol Bindings	□	■	■
Allows Service Binding Order Adjustment	□	■	■
Configuration Changes Require Reboot	□	■	□
TCP/IP Aliasing	■	■	■
TCP/IP Large Window Support	■	□	■
TCP/IP Enhanced RTT Estimation	■	□	■
TCP/IP Selective Acknowledgement Support	□	□	■
DHCP Services			
DHCP Server Service	■	■	■
IETF DDNS Standards Compliance	■	□	■
BOOTP Server Service	■	■+	■+
DHCP User Class Support	■	□	■
DHCP Statistics and Analysis Reporting	□	□	■
DHCP Fault Tolerance	□	□	■
Rogue DHCP Server Detection	■	□	■
DHCP Multicast Address Assignment	□	□	■
DHCP Vendor Class Support	□	□	■
DNS Services			
DNS Server Service	■	■	■
Dynamic DNS	■	□	■
WINS Server Service	□*	■	■
WINS Dynamic Record Deletion	□	□	■
WINS Manual Tombstoning	□	□	■
WINS Persistent Connections	□	□	■
DNS Resolver Cache	■	□	■
Remote Access and VPN Services			
Direct Dial Support	■	■	■
Virtual Private Networking Support	■	■	■
TCP/IP Protocol Support	■	■	■

IPX/SPX Protocol Support	■	■	■
NetBEUI Protocol Support	■	■	■
DHCP Addressing Support	■	■	■
Manual IP Pool Addressing Support	■	■	■
Tunneling / Point-to-Point Tunneling Support	■	■	■
IP Security Support	■	■	■
Layer 2 Tunneling Protocol (L2TP) VPN Support	□	□	■
Perfect Forward Secrecy (PFS) Support	■	□	□
Certificate Discovery Protocol (CDP) Support	■	□	□
Restartable File Copy	□	■	■
RADIUS Client Support	■	■	■
RADIUS Server Support	■	□	■
Phonebook Administration	□	■	■
Connection Sharing	□	□	■
Server-to-Server VPN Support	■	□	■
Directory Integration for Policy Management	□	□	■
Supports Callback Security	■	■	■
Password Authentication Protocol (PAP) Security	■	■	■
Challenge Handshake Authentication Protocol (CHAP)	■	■	■
Microsoft CHAP Security	□	■	■
Shiva PAP Security	□	■	■
Modem Sharing Services	□	□	■
Connections per Server	>416	256	256
Routing and WAN Services			
LAN Routing Support	■	■	■
PPP Routing Support	■	■	■
ATM Routing Support	■	□	■
X.25 Routing Support	■	■	■
Frame Relay Routing Support	■	■	■
On-Demand Connection Support	□	■	■
TCP/IP Protocol Support	■	■	■
IPX/SPX Protocol Support	■	■	■
RIP Support	■	■	■
OSPF Support	■	■	■
NLSP Support	□	□	□
TCP/IP Filtering	□*	■	■
IPX/SPX Filtering	■	■	■
DHCP Relay Support	□	□	■
DNS Proxy Support	□	□	■

IGMP Protocol Support (Multicast)	□	□	■
Network Address Translator	□*	□	■
Dynamic Bandwidth Allocation (Admission Control Service)	□*	□	■
Extensible SDK and API Set	■	■	■
Multi-link PPP Support	■	■	■
Includes SNMP Monitoring and Management Package	■	□	□
Telephony Support			
Telephony Solution Available	□	■	■
TAPI 2.0 Support	□	■	■
TAPI 3.0 Support	□	□	■
Integrated Dialer	□	□	■
ITU H.323 Conferencing Protocol Support	□	□	■
Quality of Service			
IETF RSVP (QoS) Support	■	□	■
IETF diff-serve (CoS) Support	□	□	■
QoS API Support	■	□	■

+BootP support is limited.

*These services are available in the Sun Firewall product.

Network Architecture

An operating system’s network architecture refers to its physical network device support and its ability to operate over a variety of LAN topologies. This review covers each operating system’s physical device driver architecture, driver support, driver availability, and support for the various network media types available on the market today such as Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI, and ARCnet.

Solaris 7 Implementation Details

When examining network architecture support for Solaris 7, there are three key areas to look at:

- Hardware support.
- Network media support.
- Device configuration.

Hardware Support

You are faced with two completely different sets of issues when dealing with the hardware support for Solaris 7. The first is the support on Sun’s proprietary hardware. Because Sun is a hardware company as well as a software business, the support for Sun operating systems, included packages, and licensed third-party applications is excellent. A purchaser can be assured that a choice to run Solaris 7 on Sun SPARC-family hardware will cause few if any compatibility issues between the software and the hardware. The biggest issue for compatibility on the proprietary hardware platform is which version of the Solaris operating system is being run. And there are two issues that can further confuse the Solaris user.

The first is which revision of the Solaris operating system is being run as the platform for Solaris 7. Solaris 7 is supported on both the Solaris 2.6 and Solaris 7 versions of the core operating system. While this, on the surface, may seem like only a small difference, many applications that run on Solaris 2.6 will not run or need to be recompiled to run on Solaris 7. Second, on current Sun hardware, the operating system can be installed in full 64-bit mode or as a 32-bit operating system. Some versions of the various applications that make up Solaris 7 have earlier versions in place that will only work with Solaris as a 32-bit operating system. For example, problems have been reported with PC NetLink and Solstice PPP 3.0.1. Also, 32-bit tools from third party vendors may need to be recompiled before they can run on 64-bit systems. Primarily, this problem is encountered when the tools have been compiled with a restrictive flag (-xarch=v9).

The second set of hardware issues deals with running Solaris 7 on the Solaris for Intel platform (also referred to as Solaris x86). Sun certifies compatibility on only a very small subset of the devices (systems, network adapters, SCSI controllers, etc.) that are available in the x86 world. For example, they only officially support Ethernet cards from fewer than 20 vendors (see The Solaris Hardware Compatibility Web site for the complete list of compatible hardware).

Network Media Support

All standardized network architecture types are supported as part of the operating system, including:

- Ethernet (10Base-T, 10Base-2).
- Fast Ethernet (100-BaseT).
- Gigabit Ethernet.
- Token Ring.
- FDDI.

While Sun Solaris 7 doesn’t support ARCnet, it does support native ATM. ATM technology itself is emerging as a worldwide standard for the transmission of information. Numerous telecommunications organizations and enterprise customers are rapidly deploying it today. For many, ATM represents the next generation for LAN switching. Its extremely high performance is enabling a new breed of real-time voice and video applications.

Sun Solaris 7 using SunATM adapters supports 155MB/second and 622MB/second transfer rates. At 155MB/second, data can be transferred over multimode fiber or standard category 5 cables. The ATM Forum User Network Interface 3.0, 3.1, and 4.0 specifications are also supported. In accordance with RFC 1577, TCP/IP applications can run transparently over ATM.

Device Configuration

An advantage Sun Solaris 7 has over Windows NT 4.0 is the ability to make most device configuration changes without having to reboot the system. You can, for example, reconfigure a network card without restarting the server. However, this advantage does not extend to Windows 2000 Server. Windows 2000 Server can change device configuration settings without rebooting.

An area of configuration where Sun Solaris 7 falls behind Windows 2000 is in support for Plug and Play and auto-detection of devices. While Windows 2000 supports auto-detection during and after installation of the operating system, Sun Solaris 7 only supports auto-detection of devices during installation of the operating system. This means you must manually detect and configure new devices.

Windows NT Server 4.0 Implementation Details

Windows NT Server 4.0 uses the existing 32-bit NDIS standard for network device drivers. Introduced with Windows NT 3.1, 32-bit NDIS provides support for all major types of devices including ISA, ISA PnP, PCI, EISA, MCA, and PCMCIA. Because 32-bit NDIS has been available on the marketplace for years, both hardware support and media types support is considerable, including Ethernet (10Base-T, 10Base-2), Fast Ethernet (100-BaseT), Gigabit Ethernet, ARCnet, Token Ring, and FDDI. However, Windows NT Server 4.0 does not provide native support for ATM.

On the Windows NT Server 4.0 CD-ROM, driver support is provided for most popular network cards. Additionally, any 32-bit NDIS driver can be used. Windows NT Server 4.0 will auto-detect most network cards that are supported during initial operating system installation. PCI device settings are automatically detected and configured in most cases. All other types of cards must have their configuration settings specified by hand. As with Solaris 7, all hardware-related configurations must be done outside of the operating system.

Post-installation, or in systems with multiple network cards, all devices must be added by hand. Additionally, if the device is not PCI-based, configuration settings must be manually specified. Any type of device-related configuration requires that the server be rebooted, potentially interfering with server uptime for simple configuration-related issues.

Windows 2000 Server Implementation Details

Windows 2000 Server expands on the 32-bit NDIS driver model. As with Windows NT Server 4.0, device and media type support is outstanding due to the longevity of the 32-bit NDIS driver standard. As would be expected, all standardized network architecture types are supported as part of the operating system, including:

- Ethernet (10Base-T, 10Base-2).
- Fast Ethernet (100-BaseT).
- Gigabit Ethernet.
- ARCnet.
- Token Ring.
- FDDI.

Native ATM Support

New in Windows 2000 Server is native Asynchronous Transfer Mode (ATM) support. Microsoft has entered into licensing agreements with FORE Systems and Olicom to bundle Olicom’s UNI 3.1 call manager and FORE Systems’ ForeThought ATM LAN Emulation client software with Windows 2000 Server. These provide solution developers with an additional path to bring their products to market quickly for use with Windows 2000 Server.

Plug and Play Support

Windows 2000 Server, unlike either Solaris 7 or Windows NT Server 4.0, is a Plug and Play compliant operating system. In addition, native operating system support is also provided for PCMCIA and CardBus devices. Consequently, Windows 2000 will automatically detect all ISA PnP, PCI, EISA, PCMCIA, and CardBus devices, regardless of whether a driver is present. (The user will be prompted for device drivers if one is not present as part of the operating system.) Also, unlike Solaris 7 or Windows NT Server 4.0, post-installation, Windows 2000 Server will automatically detect all of the aforementioned devices.

Additionally, because Windows 2000 supports Plug and Play, PCMCIA, and CardBus, hardware configuration settings such as I/O ports or interrupts can be managed via the operating system rather than via vendor-supplied utilities. Also, unlike either Windows NT Server 4.0 or Solaris 7, hardware conflicts will be automatically resolved by the operating system.

Dynamic Configuration Changes

Configuration changes, such as the addition or removal of device drivers, can be made without rebooting the server. In most cases, even hardware configuration settings such as changing transceiver types, can be made while the system is running, if the device supports dynamic configuration.

Power Management

Windows 2000 Server also supports all of the latest standards in power management including APM and ACPI. Consequently, network devices can be powered off when not in use and dynamically reactivated via incoming packets or outgoing traffic. Windows 2000 Server also supports Wake-on-LAN technology, allowing an entire machine to be powered down and then reactivated via incoming network requests. Although these features are probably not of benefit to most LAN administrators, they will prove beneficial to any mobile or power-conscious users. With APM and ACPI support, Windows 2000 Server has the potential to run for longer periods on battery powered systems thanks to its ability to conserve power when not in use and then to be dynamically reactivated via incoming network traffic.

Network Architecture Summary

Windows 2000 Server supports Plug and Play, hardware auto-detection and auto-configuration during installation and post installation. You can adjust hardware parameters in the operating system, and configure all network device settings dynamically without a reboot. These features are unmatched by either Solaris 7 or Microsoft Windows NT Server 4.0. Additionally, where ATM connectivity is a priority, Windows 2000 Server offers native ATM support.

Solaris 7 supports automatic detection of hardware during installation and the ability to change device settings dynamically within the operating system, but it does not support Plug –and Play. Also, the range of hardware support for the x86 platform for Solaris 7 is quite limited.

Although Windows NT Server 4.0 benefits from excellent device support and driver technology maturity, its general lack of auto-detection and auto-configuration abilities for network devices and its inability to dynamically reconfigure existing devices make it the most difficult of the three operating systems to administer. This is especially true, given the downtime generated from simple device configuration changes by the requirement of many reboots.

Network Protocol Support

Network protocol support is one of the most critical low-level features of a network operating system. It alone determines the types of clients supported by the server software as well as the types of other computer systems with which the network operating system can communicate. For the purpose of this document, each operating system will be reviewed based on its ability to provide core networking services and functionality over the TCP/IP protocol, the most dominant protocol in use today. Additionally, each network operating system will be reviewed based on its ability to support other popular network protocols, such as IPX/SPX, NetBEUI, AppleTalk, or DLC.

Solaris 7 Implementation Details

Built on and around the TCP/IP protocol, Solaris deserves its reputation as the operating system on which the Internet runs. With a robust and mature TCP/IP implementation, Solaris 7 boasts IP connectivity that is second to none. Support for Streams is also part of the base operating system. However, other protocols are not well integrated with the operating system.

Support for NetBEUI, NetBIOS, IPX/SPX, and AppleTalk is available via the TotalNET Advanced Server 5.2 application. Services are configured in three *Realms*. NetBEUI and NetBIOS support are provided via the

Services for LM-NT-OS/2 Realm, IPX support via the Services for NetWare Realm, and AppleTalk via the Services for AppleTalk realm.

Once the various protocols are installed, the services can be started and stopped dynamically and do not require a reboot to handle configuration changes.

Windows NT Server 4.0 Implementation Details

Windows NT Server 4.0 was designed to be protocol independent. Rather than having support for specific protocols built into the operating system, a modular driver architecture has been used to provide protocol support. Drivers for many popular protocols are shipped with the operating system. The protocols include:

- TCP/IP
- NetBEUI
- IPX/SPX (NWLink)
- DLC
- AppleTalk
- Streams Environment

Additionally, as modular driver architecture has been used, additional protocol support can be added easily to the operating system. However, not all protocols under Windows NT offer full networking and operating system functionality such as file and printer sharing, directory services, browsing/service location, or network name resolution. Instead, full networking functionality is offered only with the TCP/IP, NetBEUI, and IPX/SPX protocols. A subset of networking functionality is offered with the AppleTalk protocol for connectivity to client systems running Apple MacOS. DLC and Streams Environment have been provided for specialized connectivity purposes only. Point-to-Point Tunneling protocol is used extensively as a transport to carry traffic from other protocols securely over a public network as part of the Windows NT Server 4.0 Remote Access/VPN functionality, which will be discussed elsewhere in this document. Connectivity is transparent and automatic to the end user over both local and wide area network environments (with the noted exception of NetBEUI over a WAN, as it is a non-routable protocol).

Configuration at the time of installation and post-installation is GUI-based via the Network application in the Windows NT Server 4.0 control panel. Protocols can be added or deleted and selectively bound to all network interfaces present in the server. Protocol binding order is determined by the order in which the protocols were initially installed. The order can be changed at any time for each interface, allowing a greater detail of control than Solaris 7 allows. For example, the first interface could have TCP/IP and IPX/SPX both bound, with TCP/IP having precedence whereas the second interface could still have both protocols bound, but the IPX/SPX protocol could have precedence.

Additionally, network services can be selectively enabled or disabled on a per adapter or per protocol basis, or any combination thereof. This will provide extremely fine control over networking configuration. And it will allow extremely secure configurations to be constructed with a minimum of difficulty. Such configurations might include disabling all network services on public interfaces connected directly to the Internet. The only downside to this configuration is that most configuration changes require the server be rebooted.

Windows 2000 Server Implementation Details

Windows 2000 Server builds on the already strong protocol support in Windows NT Server 4.0. Basic network protocol support remains the same, although the user interface to manage network configuration has been totally revamped.

The Network application in Control Panel has been replaced with the new Network Connections folder. This allows all physical and remote access interfaces to be managed using the same user interface. It greatly simplifies network configuration for Remote Access Service (RAS). All configuration changes can now take place dynamically, eliminating the need for any server reboots to add, remove, or change network protocol support. Additionally, entire network interfaces and all associated bindings can be enabled or disabled at the click of a mouse –button without a server reboot.

TCP/IP Improvements

Basic TCP/IP protocol support has been greatly enhanced in Windows 2000 Server with the addition of several key performance improvements for networking in high-bandwidth LAN and WAN environments. Specifically, these improvements include:

- **Large Window Support** greatly improves the performance of TCP/IP when a large amount of data is present on the physical network that remains unacknowledged between two connected hosts over a long period of time. In TCP-based communications, the window size is typically fixed and negotiated at the onset of a session between two hosts. With Large Window Support, window size can be dynamically recalculated and increased as appropriate during longer sessions when large amounts of data need to be interchanged. This provides for additional data packets to be in transit on the network at one time, thereby increasing effective bandwidth.
- **Selective Acknowledgement** provides for quick and effective recovery from a state of network congestion caused by temporary interference on the physical media. Selective Acknowledgement is a TCP option that allows the receiver to selectively notify and request from the sender only those packets that were missing or corrupted during initial delivery. In prior implementations of TCP/IP, if a receiving host failed to receive a single TCP packet, the sender would be required to retransmit not only the corrupt packet, but also all packets transmitted after the missing one. With Selective Acknowledgement, only those packets actually corrupted or missing must be retransmitted.
- **RTT Estimation** improves TCP/IP performance by accurately assessing the round-trip time (RTT) interval between hosts on the network. Because performance is dependent on knowing how long to wait for a missing packet, improving the accuracy of RTT estimation results in improved timeout values being set on each host. Consequently, hosts cannot submit requests for packets to be retransmitted until the requisite time interval expires. Better timing will improve performance over long round-trip network links, such as WANs spanning large distances using wireless or satellite links.

Network Protocol Support Summary

Windows 2000 Server ties with Windows NT Server 4.0 in providing support for the greatest number of protocols (TCP/IP, IPX/SPX, NetBEUI, AppleTalk, DLC, and Streams). In Windows 2000, unlike Windows NT Server 4.0, protocol configuration can be performed dynamically, allowing settings to be changed without reboots. Additionally, for TCP/IP-based environments, Windows 2000 Server offers several performance enhancements unmatched by the other operating systems.

Basic protocol support is identical in Windows NT Server 4.0 and Windows 2000 Server. However, two key differences make Windows NT Server 4.0 a less ideal solution. Windows NT Server 4.0 does not support Windows 2000 TCP/IP performance enhancements and requires a reboot for certain configuration changes.

Solaris 7 offers excellent TCP/IP support. TCP/IP is, and always has been, the native protocol for the Sun operating system and the support for TCP/IP in the current product is a very mature and stable implementation. The TotalNET Advanced Server component of the Solaris 7 package adds support for NetBIOS, NetBEUI, AppleTalk, and IPX/SPX clients.

Dynamic Host Configuration Protocol (DHCP)

The Dynamic Host Configuration Protocol(DHCP) is the IETF's standard for centrally managed TCP/IP network addressing and host configuration. For the purpose of this review, each operating system will be reviewed on its ability to provide an IETF-compliant DHCP implementation, as well as its value-added services to ease DHCP service implementation and management.

Solaris 7 Implementation Details

Solaris 7 provides full support for the DHCP protocol as specified by the IETF's latest specifications. The Solaris 7 DHCP implementation supports the following IETF RFCs for the DHCP protocol:

- RFC 2131 – Dynamic Host Configuration Protocol.
- RFC 2132 – DHCP Options and BOOTP.

Solaris 7 also provides support for the BOOTP protocol (a predecessor of DHCP that allocated IP addresses only without any configuration information). The following RFC standards are supported:

- RFC 1497 – BOOTP Vendor Information Extensions.
- RFC 1534 – Interoperation Between DHCP and BOOTP.
- RFC 1542 – Clarifications and Extensions for the Bootstrap Protocol.

Configuration and Management

Configuration and management is handled by a number of command line tools (such as dhtadm – the DHCP configuration table management utility). Capabilities are little more than the ability to configure the server service and the address pool, and turn the service on or off.

Fault-Tolerance

Finally, no fault-tolerance features are provided as part of the Solaris Easy Access Server DHCP implementation. Consequently, if a server goes down and all leases expire, users will be unable to obtain network connectivity until the DHCP service is restored.

Sun Enterprise Server, on the other hand, includes Sun Cluster. With Sun Cluster, you can configure failover support for DHCP.

Windows NT Server 4.0 Implementation Details

Windows NT Server 4.0 provides full compatibility with the DHCP protocol as specified by the IETF's original specification for DHCP. The Windows NT Server 4.0 DHCP implementation is fully compliant with the following IETF RFCs:

- RFC 1533 – DHCP Options and BOOTP Vendor Extensions.
- RFC 1534 – Interoperation Between DHCP and BOOTP.
- RFC 1541 – Dynamic Host Configuration Protocol.
- RFC 1542 – Clarifications and Extensions to the Bootstrap Protocol.

Configuration and Management

On Windows NT Server 4.0, DHCP is managed as its own Windows NT Service. A graphical DHCP Manager utility is provided for DHCP administration. The administration utility must be run on the server console – remote

DHCP server administration is not supported. Configuration information itself is stored in a Microsoft Jet-derived database. Command line utilities are provided for the backup and maintenance of this database.

DHCP support has existed on Windows NT Server since the product's inception with Windows NT Advanced Server 3.1. Because the implementation has remained largely unchanged, upgrades from prior versions are a non-issue for Windows NT Server customers.

Fault-Tolerance

No fault-tolerance features are provided with the Windows NT Server 4.0 DHCP implementation. Consequently, if a DHCP server fails and all leases expire, users will be unable to obtain network connectivity until the DHCP service is restored.

Windows 2000 Server DHCP Implementation Details

Windows 2000 Server improves on the Windows NT Server 4.0 DHCP implementation It supports all of the latest IETF specifications for the protocol. At the most basic level, full support for the following IETF RFCs is provided:

- RFC 2131 – Dynamic Host Configuration Protocol.
- RFC 2132 - DHCP Options and BOOTP Vendor Extensions.
- RFC 1534 – Interoperation Between DHCP and BOOTP.
- RFC 1542 – Clarifications and Extensions to the Bootstrap Protocol.

For those unfamiliar with the current status of DHCP, RFC 2131 officially supercedes RFC 1541, which was used as the basis of the Windows NT Server 4.0 DHCP implementation.

Additionally, for Windows 2000 Server, many new features have been added to the DHCP service support. Most important is the addition of enhanced monitoring and statistical reporting capabilities to the DHCP manager utility. Specifically, the DHCP server will now provide notification when IP addresses are running below a user-defined threshold. For example, an alert could be triggered when 90 percent of the IP addresses available have been assigned. A second, escalated alert could then be triggered when the available IP address pool is exhausted.

Configuration and Management

The DHCP Manager now provides graphical display of statistical data. This helps administrators monitor DHCP system status, such as the number of available versus depleted addresses, or the number of leases being processed per second. Additional statistical information includes the number of messages and offers processed. It also includes the number of requests, acknowledgements, declines, negative acknowledgements (NACKs), and releases received. The total number of scopes and addresses on the server, the number used, and the number available are also displayed. These statistics can be provided for a particular scope or at the server level, showing the aggregate of all scopes managed by that server.

Vendor Specific Options

Vendor specific options and user class support has also been added in Windows 2000 Server DHCP implementation. Vendor classes are defined by specific vendors and are triggered by data bits that determine whether a given option class is standard or vendor-specific. Once identified as vendor-specific, DHCP looks up the configuration as specified, enabling compelling custom applications for enterprise networks to be introduced quickly. Vendor class and vendor options are currently undergoing evaluation by the IETF and are described in RFC 2132.

User Class Support

User class support is also provided as part of the Windows 2000 Server DHCP implementation. This allows DHCP clients to specify the type of client they are, allowing for customized configurations to be easily dispatched. This provides the systems administrator with a greater degree of flexibility than available in either the Solaris 7 or Windows NT Server 4.0 DHCP implementation. For example, laptop clients could be assigned shorter leases than desktop clients. If user class settings are left unused, default settings are assigned.

Multicast Support

Multicast addresses can now be assigned, in addition to unicast addresses, by the DHCP service in Windows 2000 Server. A proposed IETF standard is used as the basis for multicast address allocation. This benefits systems administrators by allowing multicast addresses to be assigned and managed in the same fashion as unicast addresses, allowing for complete leverage of the existing DHCP infrastructure. Multicast support is composed of two parts. The first is the server component, where multicast scopes and IP address ranges are created and managed just as if they were unicast addresses. The second component is a set of customizable client-side APIs, which are used within the customer's application to request, renew, and release multicast addresses. This provides a considerable benefit to customers developing multicast applications, such as streaming media-based solutions.

Rouge DHCP Server Detection

Rogue DHCP server detection support has been added in Windows 2000 Server. With this feature, rogue or inadvertently configured DHCP servers will be unable to create address assignment conflicts on customer's networks. This feature is implemented through the Active Directory service. A list of authorized servers in Active Directory is maintained. If an unauthorized server comes online, it will not receive an authorization from the directory and will not allow itself to process client requests. If a server comes up that is in a workgroup rather than being a domain member, the server will send out a DHCPINFORM broadcast. If a registered DHCP server is online and acknowledges the workgroup DHCP server, the workgroup DHCP server will treat itself as rogue and not process client requests. If no registered servers are online when the workgroup DHCP server comes online, DHCPINFORM broadcasts are automatically sent every five minutes. This allows the workgroup DHCP server to be classified as rogue and stop servicing requests if a registered server comes online.

Fault-Tolerance

Windows 2000 Server Clustering Services, available in Windows 2000 Advanced Server, provide the foundation for fully redundant, fault-tolerant DHCP services. Clustering Services, when used with DHCP, can provide for significantly higher availability, easier manageability, and greater scalability than would otherwise be available. The DHCP server service can now be run natively as an application on top of Clustering Services, with the DHCP configuration database stored on the cluster's shared disk array. If a failure occurs on the first node in the cluster, the name space and all services are transparently moved to the second node. This means that there will be no changes for the client, which will see the same IP address for the clustered DHCP server. Unlike Windows NT Server 4.0 or Solaris 7 implementations, DHCP services will remain totally uninterrupted in the event of a system failure.

DHCP Client Support

DHCP client support has also been improved in Windows 2000 Server. Previously, if a client were brought online and a DHCP server were unavailable, the machine would not have the TCP/IP protocol configured. With Windows 2000, the DHCP client service uses a two-step process to configure the client, ensuring that the TCP/IP stack is fully initialized. When a machine is booted, it will first attempt to locate a DHCP server. If this fails, it will automatically configure itself with a selected IP address. If the client had a previously obtained lease, the client will try to ping the default gateway listed in the lease. If it is successful, it assumes that the client has not been moved and continues to use that same lease. The client will then continue to try to renew the lease until a DHCP server becomes available. If the ping fails, the client assumes that there are no DHCP services available and automatically configures itself. It will then automatically keep trying to reconfigure itself every five minutes until a DHCP server comes online.

DHCP Summary

The Windows 2000 Server implementation of DHCP contains true monitoring and statistical analysis capabilities, making it easy to track for the system administrator. Many other benefits are added, including vendor and user classes, rogue DHCP server detection, fault tolerance via Clustering Services, and automatic client configuration. Such features are , unequaled in Windows NT Server 4.0 or Solaris 7. For the enterprise customer where availability is paramount, rogue DHCP server detection and support for Clustering Services are extremely important. These two features virtually guarantee protection from either rogue servers or system failures.

The Solaris 7 DHCP implementation lacks many of the features found in Windows 2000. However, by offering the Dynamic BOOTP feature in addition to basic DHCP services, it provides a more full-featured solution than Windows NT 4.0. Dynamic BOOTP will prove to be of considerable use in environments where not every client is DHCP-enabled and where systems administrators manage the network via central IP address allocation.

Of the three implementations, Windows NT Server 4.0 DHCP service is the most dated. It offers nothing in the area of fault tolerance and no features beyond basic RFC compliance. Additionally, because Windows NT Server 4.0 shipped an entire generation before Windows 2000 Server, it is only compliant with the original DHCP specifications, rather than the current specifications.

Name Resolution

The Domain Name Service (DNS) is the IETF’s standard for providing name resolution over the TCP/IP protocol. Alternatively, for NetBIOS networks running the TCP/IP protocol, the Windows Internet Naming Service (WINS) is the IETF’s standard for providing additional name resolution capabilities. This paper will review each network operating system’s ability to provide a standards-compliant, operating system-integrated DNS implementation. Additionally, each operating system will be evaluated on its ability to provide value-added services to enhance the deployment and management of the DNS implementation.

Solaris 7 Implementation Details

Solaris 7 provides full support for the Domain Name Service (DNS). The Solaris 7 DNS implementation is fully compatible with BIND 4.9.3 and all current IETF RFCs that cover DNS. But DNS is not the primary name service for Solaris 7. That role is the responsibility of the Network Information Service + (NIS+), which is discussed later under “Management and Directory Services.”

DNS configuration can be managed through the Solaris Administration wizards. These administration wizards are run through the Solaris Management Console or from the command line. The DNS Server Configuration wizard is used to configure DNS servers. The DNS Client Configuration wizard is used to configure DNS clients. Both wizards have a fairly efficient graphical user interface that allows you to configure DNS.

When running Solaris PC NetLink and emulating a Windows NT domain controller, Solaris 7 provides full support for WINS. This support is the same as that provided in Windows NT Server 4.0.

Windows NT Server 4.0 Implementation Details

Microsoft Windows NT Server 4.0 provides two name resolution facilities – standard DNS and the Windows Internet Naming Service (WINS). The DNS implementation is relatively standardized and provided interoperability between Windows NT 4.0-based machines running TCP/IP and the Internet. WINS provided additional name resolution capabilities for NetBIOS-based computer systems running on top of the TCP/IP protocol.

Standards Support

The DNS implementation represents a relatively standardized implementation of BIND 4.9, conforming to IETF RFCs 1034 and 1035. DNS information is stored in an ASCII-text based database in BIND 4.9 format. Administration is accomplished either using a GUI-based tool, the DNS Manager, or by editing the ASCII-text databases directly using a text editor.

As with BIND 4.9, the Windows NT Server 4.0 DNS implementation can serve as either a primary or secondary name server for any given zone. Interoperability with other DNS servers is also provided as with any BIND 4.9 implementation.

WINS Support

WINS is an implementation of the IETF standards for providing NetBIOS browsing and name resolution over the TCP/IP protocol, as defined in RFCs 1001 and 1002., In addition to providing machine name and TCP/IP address mapping, it helps provide browsing and service location for such things as domain controllers and workgroups. WINS allows for dynamic updates and provides for full interoperability with the DHCP protocol for instant machine name and TCP/IP address mappings.

The DNS and WINS server implementations are fully integrated to provide some dynamic DNS capabilities. Any Windows NT Server 4.0 DNS server that is the primary name server for a given zone can reference the WINS database, providing instant, dynamic DNS updates via WINS.

Windows 2000 Server Implementation Details

Microsoft Windows 2000 Server improves on the functionality of the name resolution services from Microsoft Windows NT Server 4.0.onIt offers a highly enhanced name resolution solution.

Standards Support

The DNS implementation in Windows 2000 Server has been totally reworked to take advantage of Active Directory services and to provide support for the latest IETF standards for the management of dynamic addresses and name resolution. At the standards level, the DNS implementation remains based on the IETF RFCs 1034 and 1035. However, additional support for the official IETF working draft of the Dynamic DNS update – RFC 2136 – has been provided.

Configuration and Management

Management of DNS services is now performed entirely through the new Microsoft Management Console (MMC), making administration considerably easier. MMC provides a consistent look with other Windows 2000 management packages. For the first time, remote management of DNS servers is supported via MMC. Wizards have been added to the MMC, making DNS configuration easier than it is on other platforms.

Dynamic DNS

Windows 2000 Server also supports Dynamic DNS, providing instant DNS registration for DHCP-configured hosts. Unlike other implementations, Windows 2000 Server is based on the proposed IETF standard and therefore will interoperate with other dynamic DNS systems as they become available.

DNS Resolver Cache

A DNS Resolver Cache service also has been added to speed DNS queries. This service greatly reduces DNS network traffic, and speeds name resolution by providing a local cache for DNS queries on all Windows 2000-based servers.

Directory Integration

Finally, the DNS service has been fully integrated with Active Directory, which natively uses the Windows 2000 Server DNS implementation as its naming resolution service. Domain names on Windows 2000 Server are now DNS domain names. Consequently, “Microsoft.com” is a valid DNS domain and is also a valid Active Directory domain; the two are one and the same. Tight directory integration means that the Active Directory fits naturally into intranet environments and the Internet. There is no additional overhead or effort required to manage DNS.

When Active Directory is installed on a server, it publishes itself via Dynamic DNS. All DNS information is stored using the Active Directory client/server database engine (based on the Microsoft ESE97 engine), providing a significantly higher level of performance and database reliability than is available with text-based databases. (Non-Active Directory DNS implementations still use the BIND 4.9 text-based database format.) DNS information can be automatically replicated to other DNS servers throughout the Active Directory organization, providing additional levels of fault-tolerance. Finally, the DNS database can be physically configured in a true hierarchy. This will allow each workgroup to seamlessly manage its portion of DNS. It eliminates the need to have the entire DNS database replicated in full throughout an organization, and it provides transparent access to the end users with no need to reference specific DNS servers.

WINS Support

The WINS services are enhanced in Windows 2000 Server to continue to provide NetBIOS-based TCP/IP name resolution services. New features include Persistent Connections, Manual Tombstoning, MMC-based management, enhanced filtering and record searching, dynamic record deletion and multi-select, and record verification and version number validation.

Persistent Connections allow each WINS server to maintain a dedicated connection with one or more replication partners, eliminating the overhead of opening and closing connections. The benefit to users is improved replication speed. Manual Tombstoning allows for a tombstone marker for deleted records to be propagated to all WINS servers. This prevents undeleted record copies from reappearing on other WINS servers and then being re-propagated back into the network. MMC is now used for all WINS management, providing a more user-friendly and powerful environment for administrators.

Administrators can now search for records of interest by showing only those that fit a specific criterion through the new MMC tool. The user interface has also been improved to allow dynamic records to be manually deleted (this was previously not possible). Multiple deletions can be made simultaneously. Finally, new tools verify consistency between WINS servers, allowing systems administrators to monitor the enterprise more accurately.

Name Resolution Summary

Windows 2000 Server supports both DNS and WINS. Both naming services are compliant with all of the latest IETF RFCs. Dynamic DNS and DHCP integration is fully supported and implemented according to the latest IETF specifications. The MMC-based management tools provide an easy-to-use graphical user interface for managing name resolution services and are also well-suited for novice administrators.

Solaris 7 offers a comprehensive DNS facility that is standards-based. While Solaris 7 supports current IETF RFCs related to DNS, it does not support dynamic DNS technology at this time. Additionally, SOLARIS 7 does not provide native support for WINS. WINS support is only available through Solaris PC NetLink.

Windows NT Server 4.0 name resolution services represents the most dated of the three operating systems. Both DNS and WINS are supported and both implementations are in compliance with IETF specifications. The DNS implementation is merely an implementation of BIND 4.9 with a GUI management tool – no additional features or capabilities such as Dynamic DNS are present. WINS and DNS can be integrated to provide pseudo-Dynamic DNS functionality, but this is a rather limited and non-standardized solution. Additionally, although adequate, the GUI management tools are an entire generation behind Windows 2000 Server in ease-of-use and functionality.

Remote Access and VPN Support

Telecommuting and traveling for business are commonplace in today's global economy. For both of these to be effective, remote access to the corporate network is a must. A network operating system should provide full remote access capabilities. A core feature set at minimum should include support for modem and ISDN dial-up users, support for the PPP protocol, multi-protocol (IPX and TCP/IP support), callback, and encrypted login. Additionally, connection management software, shared modems for internal dial-out, and a VPN solution for secure access over the Internet are nice-to-have features.

Solaris 7 Implementation Details

Solaris 7 has two key remote access and VPN components:

- Solstice PPP
- SunScreen SKIP

These components support Solaris clients only.

Remote Access Support

Solaris 7 provides a remote access implementation through the inclusion of the Solstice PPP 3.0.1 application. Solstice PPP provides a standard implementation of the following IETF RFCs:

- RFC 1661 - Point-to-Point Protocol (PPP) - Describes a standard method for transporting multiprotocol datagrams over serial point-to-point links.
- RFC 1662 - PPP in HDLC-like Framing - Describes the use of HDLC-like framing for PPP encapsulated packets.
- RFC 1332 - PPP Internet Protocol Control Protocol (IPCP) - Describes the Network Control Protocol (NCP) for establishing and configuring the Internet Protocol (IP) over PPP, and a method for negotiating the use of Van Jacobson TCP/IP header compression with PPP.
- RFC 1334 - PPP Authentication Protocols - Describes two protocols for user authentication in the PPP domain: the Password Authentication Protocol (PAP) and the Challenge-Handshake Authentication Protocol (CHAP).
- RFC 1144 - Compressing TCP/IP Headers for Low-Speed Serial Links - Describes a method to improve the performance of TCP/IP connections across low-speed links by compressing the packet headers.

Management for the Solstice PPP 3.01 dial-up networking service is provided by a combination of command-line tools that provide diagnostic and statistical information (ppptrace and pppstat), and by the manual editing of the PPP configuration files for the server and client system.

VPN Support

For VPN services, Solaris 7 includes SunScreen SKIP. SunScreen SKIP is a subcomponent of the larger SunScreen Secure Net firewall available from Sun. Simple Key-management for Internet Protocols (SKIP) is used to manage IP encryption through a combination of shared-key and public-key encryption technologies.

SunScreen SKIP operates at the network (IP) layer and enables secure communications with all IP applications over TCP and UDP. Encryption is a key component of the SunScreen SKIP security model. SKIP supports shared keys, public keys, and certificates as well as 40-bit RC2, 40-bit RC4, 56-bit DES CBC, 128-bit RC4, 128-bit SAFER CBC and 3-key Triple-DES encryption.

SunScreen SKIP also supports automatic key distribution through the Diffie-Hellman key exchange algorithm. With Diffie-Hellman key exchange, SunScreen SKIP can securely distribute keys without needing to distribute secret keys. Once a user’s private and public key is obtained, SunScreen SKIP creates a public key certificate for the user and this certificate can then be exchanged between hosts. Through Certificate Discovery, computers running SKIP can retrieve certificates from other computers running SKIP, provided a network or serial connection is available.

SunScreen SKIP also uses Perfect Forward Secrecy (PFS) to encrypt traffic keys. With Perfect Forward Secrecy, a clock-based master key takes the place of the Diffie-Hellman shared secret key. Perfect Forward Secrecy requires that the date, time and time zone on computers be synchronized. If they aren’t, the time variable calculated for PFS would be off between hosts and decryption would fail.

Encryption is only one part of the SunScreen SKIP security model; SunScreen SKIP also supports access control lists, authentication and proxies. Access control lists restrict access to computers by IP address, host name and/or network ID. Authentication is the process that verifies computers sending messages and computers receiving messages are who they say they are. Validation of message traffic is also a part of authentication. Here, SKIP validates that the message traffic hasn’t been modified during transmission.

SunScreen SKIP also supports security proxies which are used in IP tunneling. With tunneling, a security proxy acts as the middleman to hide the corporate network topology from the outside world. Packets are sent to and received by the security proxy, which in turn passes the packets on to their final destination. In the complete security offering from Sun, called SunScreen Secure Net, other types of proxies are also supported. These proxies handle HTTP, FTP, Telnet and SMTP traffic.

Management of SunScreen SKIP is handled through a combination of graphical and command-line tools. Access control lists are managed through SunScreen SKIP Access Manager and other core functions can be managed through Skiptool. While a graphical wizard is provided for installation, configuring SunScreen SKIP is very complex.

Windows NT Server 4.0 Implementation Details

Windows NT Server 4.0 ships with a complete remote access solution including dial-up and secure VPN access. Either configuration supports both direct-dial and VPN based remote access for clients-to-server connections. Windows NT Server also provides support for server-to-server direct-dial and VPN connections.

Hardware and Protocol Support

Windows NT Server 4.0 supports dial-in clients using standard modems, ISDN, or X.25. The Point-to-Point protocol is used for remote connections and the TCP/IP, IPX, and NetBEUI protocols are all supported for dial-in. TCP/IP configuration is either on a pool basis or DHCP services can be used. Multi-link PPP is fully supported, allowing for the combination of a single logical interface from multiple physical interfaces to provide a larger pipe, increasing effective bandwidth. Concurrent connection support is limited to 256 per server.

Client Support

Auto-dial and auto-logon dial is also supported as part of Microsoft's remote access client implementation in Windows 95, Windows 98 and Windows NT 4.0. With this feature, Windows can map and maintain an association between a Dial-Up-Networking entry and a network address. It can seamlessly integrate Dial-Up Networking with files and association. If a user attempts to open a file that is only remotely accessible, the connection will be automatically dialed and established.

Restartable File Copy

Windows NT Server also supports a feature called Restartable File Copy. When downloading files from a Windows NT-based server, if the connection is interrupted during a file copy, the copy can be resumed from where the download let off rather than having to start over.

Authentication and Security

By default, remote authentication occurs in the Windows NT Domain or Workgroup in which the remote access server is a member. Users are required to have valid Windows NT user accounts with remote access permissions. RADIUS client support has also been provided as part of the remote access client. This allows authentication into ISP networks or non-Windows corporate direct-dial networks without using the Windows NT account database. With the Windows NT Option Pack, Microsoft has also provided support for a RADIUS server so that ISPs and non-Windows-based client systems can authenticate against the Windows NT Server domain.

Virtual Private Networking

Windows NT Server also provides a complete inbound and outbound VPN implementation for both client-to-server and server-to server via the Point-to-Point Tunneling Protocol (PPTP). In client-to-server VPN, clients can remotely establish connections over the Internet from their location to the Windows NT enterprise via a secure, encrypted tunnel. All standard remote access options, such as password configuration and access restrictions, also apply to PPTP clients.

Windows NT Server 4.0 also provides server-to-server PPTP support. This enables entire networks to be connected to each other securely over the Internet, rather than via more expensive dedicated leased line arrangements. This provides tremendous cost and infrastructure savings to the customer.

Management

Management of the Windows NT Server 4.0 remote access implementation is entirely GUI-based. Management tasks are accomplished via the Network application in Control Panel and the Routing and Remote Access Service Administrator application that is provided with the Windows NT Option Pack upgrade.

With the installation of the Windows NT Option Pack, Windows NT Server is also able to provide a distributed remote access phonebook solution. With the Connection Manager Administration Kit (CMAK), system administrators can customize the user interface of the remote client software and then distribute it to end-users. ISPs can maintain a POP phonebook independently of the corporate direct-dial numbers. When users connect, phonebooks from the ISP(s) and corporate network are synchronized and collated into a common view.

Windows 2000 Server Implementation Details

Windows 2000 Server improves on the Routing and Remote Access Services found in Windows NT Server 4.0on. Enhancements have been made in management tools, VPN support, policy and security management, RADIUS support, and directory integration.

Virtual Private Networking

Many enhancements have been made to the Windows 2000 Server VPN implementation. Unlike the previous version, which supported only PPTP, the Windows 2000 Server VPN implementation also supports Layer 2 Tunneling Protocol (L2TP) with IP Security Protocol (IPSEC). With IPSEC, TCP/IP traffic is encrypted using public key encryption as an alternative to PPTP for secure VPN communications. If protocols other than TCP/IP, such as NetBEUI and IPX, are to be used, then L2TP with IPSEC support can encapsulate the legacy protocol within IPSEC encrypted TCP/IP packets. Alternatively, PPTP is still available for companies who cannot justify the expense of a public key infrastructure or who want to protect their existing investment in PPTP-derived solutions.

Directory Integration

Windows 2000 Server remote access services are now fully integrated with the Active Directory service. This allows the creation of directory-based group policies for full-featured control of remote access protocols, time of use, type of use, encryption, and authentication. Consequently, support for Active Directory and the addition of the directory-integrated policy and security management enhancements effectively tackles one of the toughest administrative problems for remote connections while simultaneously reducing costs and improving security.

RADIUS Support

RADIUS support is greatly improved in the Windows 2000 Server remote access implementation. The scope of support is expanded to support both RADIUS authentication and RADIUS accounting, with information stored in either Active Directory or a local database (for workgroup servers). This allows for integrated authentication between an organization and ISP, providing for a single logon to the Internet and the VPN simultaneously. Previously, using the Internet to access a VPN connection, required a login to the Internet using an ISP account and then a login to the corporate network with an internal user account. With complete RADIUS authentication support, the ISP can setup a proxy authentication scheme in which the user can authenticate directly into an Active Directory-based system via the RADIUS protocol. Active Directory users with appropriate permissions will automatically have an account with the ISP. Users can simultaneously login to the ISP and the VPN with a single logon. Potential benefits, beyond simplified VPN login for users, include cost benefits to the customer depending on billing and service programs from the ISP.

Connection Sharing

Connection sharing is another beneficial feature added to the remote access implementation in Windows 2000 Server. With this, any network connection can be shared among users in a workgroup. Shared connections can be dynamically established without the client system needing to know the details of the connection configuration. For example, a small office could easily share a single dialup ISP connection with multiple clients without the need to setup a proxy server. Benefits to the customer are many – security is improved as fewer external connections are required to the Internet, and ISP fees can be saved by not needing to acquire separate accounts for multiple workstations.

Management

Management tools have been upgraded to support the Microsoft Management Console (MMC). Additionally, many wizards have been added to help get the system up and running quickly – automating many common administrative tasks.

Remote Access and VPN Summary

Windows 2000 Server offers the most in terms of the number of ports supported (a tie with Windows NT Server 4.0 at 256), features and functionality, and security. Its IPSEC, L2TP, connection sharing, directory integration/security policies, and RADIUS authentication support are unmatched by either Windows NT Server 4.0 or Solaris 7.

Windows NT Server 4.0 offers a considerably greater feature depth over Solaris 7 – offering VPN services, additional protocol support, RADIUS client support, additional password encryption options, and Restartable File copy. However, it falls behind Windows 2000 Server in its lack of advanced VPN, security, and connectivity features.

Solaris 7 provides remote access and VPN support via two included applications; Solstice PPP 3.01 for dial-up services and Sunscreen SKIP for VPN services. Both are strong offerings but are inherently complex to configure and manage. While Solaris 7 supports IP security and point-to-point tunneling, the implementation requires all computers involved to install and use Sunscreen SKIP. The Windows solution, on the other hand, is built on IPSEC, PPTP, and L2TP standards.

Routing and Wide Area Network Support

The ability to use a standard server and a network operating system to link local area networks or provide wide area connectivity in lieu of a traditional hardware router is becoming a priority for many customers in today's marketplace. By using standard servers rather than dedicated routers, customers can save money by avoiding purchase of separate routers. Features to look for in network operating system-based routing solutions include routable protocol support, LAN and WAN media support, multicast support, routing protocol support, management tools, and network address translation capabilities. In general, the more capabilities a routing solution has, the better the quality will be compared with a traditional router.

Solaris 7 Implementation Details

Routing is a standard component of the Solaris operating system. Solaris 7 supports multi-protocol routing services through a variety of command-line tools. The only components of routing or network configuration that can be configured through a graphical tool are default routers and network connection configuration settings. These tasks are handled through the Default Router Modification and the Network Connection Configuration administration wizards respectively.

Solaris supports a wide variety of industry-standard LAN and WAN cards. Though this list is not very extensive, physical media support is available for all major network architectures. For LANs, Solaris supports Ethernet, Fast Ethernet, Gigabit Ethernet and FDDI. For WANs, Solaris supports Frame Relay, ISDN, and X.25. Solaris also features native support for ATM.

Routing is supported for both TCP/IP and IPX/SPX. While Solaris 7 does support IPX/SPX filtering, TCP/IP filtering is only available through add-ons such as SunScreen Secure Net. Both distance vector and link state routing protocols are supported. For distance vector support, the RIP protocol is provided for IPX and TCP/IP. For link state routing protocols, OSPF is provided for the TCP/IP protocol suite. Unlike Windows 2000, Solaris 7 doesn't support IGMP for multicasting but does provide support for IPv4 and IPv6 multicasting. Other features included with Solaris 7 routing include support for routing APIs, multi-link PPP, and SNMP monitoring.

Windows NT Server 4.0 Implementation Details

Multi-protocol routing services for Windows NT Server 4.0 are provided as part of the Routing and Remote Access (RRAS) upgrade, available through a Web download to Windows NT Server 4.0 customers. RRAS provides a complete routing solution for Windows NT 4.0 that is fully integrated with Windows NT Server 4.0 networking support. An unlimited port license is included with this upgrade.

Windows NT Server routing can use all industry-standard LAN and WAN cards. Consequently, physical media support includes all major LAN networks such as Ethernet, Fast Ethernet, FDDI, and ARCnet. All major WAN connectivity options are supported including Frame Relay, ISDN, and X.25. All support is offered natively without requiring the installation and configuration of special modules for WAN connectivity.

Routing is supported for both the TCP/IP and the IPX/SPX protocols. Both distance vector and link state routing protocols are supported. For distance vector support, the RIP protocol is provided for IPX and RIP v2 for TCP/IP. For link state routing protocols, OSPF is provided for the TCP/IP protocol.

Other features included with Windows NT routing include support for on-demand links, packet filtering, routing APIs, multi-link PPP, and DHCP relay support. TCP/IP multicast support and bandwidth allocation are not provided by this version.

On-demand routing provides interfaces that will automatically dial and maintain connections only when needed. When there is no traffic, they remain disconnected. This provides a considerable benefit to customers, as it has the potential to greatly reduce telecommunications surcharges by not having to keep a link active all of the time.

Full packet-filtering support is provided for both the TCP/IP and IPX protocols. Filtering options for TCP/IP allow restriction of traffic based on TCP Port, UDP Port, IP protocol ID, ICMP type, ICMP code, source address, destination address, and TCP establishment status. IPX filtering options include restrictions based on source address, source node, source socket, destination address, destination node, destination socket, and packet type. Windows NT Server packet filters are configured on an exception basis. Filters can be configured to pass only packets from routes specified by the network manager, or they can be configured to pass everything except packets from specified routes.

Microsoft offers a complete software developer kit (SDK) for independent vendors wishing to develop solutions around Windows NT Server-based routing. The SDK provides complete documentation on the extensible application programming interfaces (APIs) included with Windows NT Server-based routing. The benefit to customers is a wider variety of solutions available for Windows NT Server and investment protection.

When using PPP connections to provide WAN connectivity, such as modems or ISDN devices, a new feature entitled multi-link PPP provides the ability to greatly enhance performance and available bandwidth at a reasonable cost. Specifically, low cost PPP links can be combined to create one larger, aggregate pipe over which routing can be enabled. For example, two 28.8 Kbps PPP dialup links could be combined to create an aggregate pipe of 56 Kbps in bandwidth.

The DHCP Relay Agent feature included with Windows NT Server allows DHCP services to function over remote network links. By default, DHCP servers can only issue TCP/IP addresses and configuration information to machines on the local network. With the DHCP Relay Agent, DHCP assignments can be made across routed networks regardless of whether the connection is made via LAN or WAN links. The benefit to system administrators is tremendous, as it allows fewer DHCP servers and less administrative overhead.

Management of Windows NT Server routing is provided through its own GUI-based administration tools and the Network application in Control Panel. Because it uses tools that look similar to other components, administration and setup is easy and familiar to the Windows NT administrator. Wizards are provided to help configure Windows NT routing for novice administrators. The RouteMon command-line scripting utility eases the configuration of interfaces, routing protocols, filters, and routes for routers running the service. It also displays the current configuration and allows batch processing and execution. Finally, SNMP management support is provided, allowing Windows NT Server routing services to be managed via popular SNMP packages such as HP OpenView.

Windows 2000 Server Implementation Details

Windows 2000 Server improves on the routing implementation in Windows NT Server 4.0on. New features for the routing services suite includes IGMP version 2 support, DNS proxy support, network address translation (NAT), an MMC-based interface, and dynamic bandwidth allocation.

New for Windows 2000 Server is native ATM connectivity. With ATM support built directly into the operating system, Windows 2000 Server provides connectivity over ATM in addition to all of the other types of WAN links supported by Windows NT Server 4.0.

IGMP, or the Internet Group Management Protocol, is used to register TCP/IP clients within multicast communication sessions. IGMP version 2 is fully supported by Windows 2000 Server. This allows subnets to use Windows 2000 Server for multicast routing, and it provides for multiple clients to share a common multicast session, improving performance and reducing costs in branch office networks.

The DNS Proxy support feature forwards DNS name queries from client computers on a private IP network to an Internet-based DNS server. This enhances security through network hiding while simultaneously supporting interoperable IETF standards for name resolution.

The Network Address Translator (NAT) provides TCP/IP address translation services between a private and a public network by rewriting packets to physically translate the TCP/IP addresses. NAT services provide many benefits to the system administrator. Most important is the reduced risk of denial of service attacks against internal systems when all internal network structures are hidden. Additionally, IP address registration costs less because customers use unregistered IP addresses internally, with translation to a small number of registered IP addresses externally.

Dynamic bandwidth allocation is offered in Windows 2000 Server in the form of the Admission Control Service (ACS). With ACS, system administrators can control the amount of bandwidth that applications can reserve. The limits are imposed via policies configured in Active Directory. This prevents any one application from overrunning the network or WAN connection, ensuring that all traffic can get through.

Finally, all GUI management tools have been upgraded to use the Microsoft Management Console (MMC). This provides a consistent user interface, making it easier for system administrators to navigate and control networking services. It reduces administrative costs and simplifies the management of networking services.

Routing and Wide Area Network Summary

Solaris 7, Windows NT Server 4.0 Routing and Remote Access Services, and Windows 2000 Server Routing and Remote Access Services are all provide a similarly strong set of routing features. All three can route the TCP/IP protocol and IPX using either the RIP or OSPF protocols. All three can route over all popular network media and WAN connections. All three offer GUI, command line, and SNMP management options.

However, Windows 2000 Server Routing and Remote Access service offers an easy-to-use and full-featured multi-protocol routing implementation. It includes network address translation, dynamic bandwidth allocation, a DNS proxy, and IGMP/multicast support. All these features provide significant administrative benefits, making Windows 2000 the best overall option.

Windows NT Server 4.0 Routing and Remote Access Service is a good mid-range entry. It contains a full range of network medium and routing protocol supports. And it offers an excellent set of management tools. However, its lack of native ATM support, which is found in both the Solaris 7 and Windows 2000 Server solution, makes it a poor choice for customers using that technology.

Solaris 7 represents the most feature-poor entry of the three. It does not feature DHCP relay services, nor on-demand connection support. These features are present in both Windows-based implementations. Additionally, its filtering capabilities are not nearly as sophisticated as those in either of the Windows-based solutions. It also lacks an extensible, published API set, so it does not have the support of the third party, independent software vendor community.

Telephony Services

For many organizations, connectivity between computer and telephone systems is a key initiative. There are many benefits in terms of integration and additional functionality. Computer telephony solutions offer a means to full integration between network operating systems and a traditional PBX-style telephone system. This document will evaluate each network operating system's on integrated telephony capabilities. It will also evaluate each system's ability as an extensible platform on which software developers can build customized solutions.

Solaris 7 Implementation Details

Solaris 7 offers no telephony protocol or API support as part of the operating system at this time, requiring the use of other operating systems or third party solutions for telephony support.

Windows NT Server 4.0 Implementation Details

Windows NT Server 4.0 represents Microsoft's entry into telephony-enabled operating systems. Telephony support is provided by the inclusion of Microsoft Telephony API (TAPI) 2.0 as part of the operating system. TAPI 2.0 abstracts the hardware layer, providing customers with freedom and device independence. Using TAPI 2.0, developers can easily write applications for use on PSTN, ISDN, PBX, and IP networks. A set of Microsoft ActiveX® controls, such as the Visual Call Control, are included with the TAPI 2.0 implementation to provide developers with a starting ground, further simplifying and accelerating the process of creating telephony-enabled applications.

Because TAPI 2.0 is integrated with Windows NT Server 4.0, it has a lower cost of development and ownership than proprietary telephony solutions because it can leverage the extremely large installed base of Windows developers and users and the associated support networks. Additionally, TAPI-derived solutions have the benefit of being able to fully integrate with the Windows operating system and Windows-based applications themselves – something that is not achievable with other proprietary telephony solutions.

Windows 2000 Server Implementation Details

Windows 2000 Server features full telephony support in the operating system, improving on the foundation in Windows NT Server 4.0. Full support for the next-generation Telephony API (TAPI) 3.0 and the ITU H.323 electronic conferencing protocol is provided. Additionally, Windows 2000 comes with an integrated Dialer application and the Microsoft NetMeeting® electronic conferencing software, providing rudimentary applications in the box that can easily be used as the basis for developing and deploying more sophisticated telephony applications. TAPI 3.0 provides the basis to unify IP and traditional telephony to enable developers to create a new breed of powerful telephony-enabled applications.

Usage scenarios abound for TAPI 3.0-based telephony applications running on Windows 2000 Server, especially when combined with other operating system features such as Active Directory, Windows Media Services, Microsoft NetMeeting, or Information Locator Services. Possible scenarios include using Windows 2000 Server as a call control platform, as a platform for an open PBX, to network enable traditional PBXs, to support voice over data networks, or to integrate voice and video dialing.

In the call control scenario, TAPI 3.0 can be used to build integrated streaming media and call control services solutions. These solutions can create sophisticated Interactive Voice Response (IVR), Intelligent Automatic Call Distributor (ACD), and skills-based routing solutions. Connecting a Windows 2000 Server with a PBX using these services creates a complete solution to allow customers and employees to access electronic information by phone.

Windows 2000 Server also makes an excellent, full-featured platform on which to build an open PBX-based system. An open PBX allows the customer to consolidate voice services and telephone switching into a single platform, thereby reducing the cost of integrating telephone and data networks. By simply adding telephone-switching cards to an open-standard PC platform with Windows 2000 Server, customers can glean the full benefit from a cost-effective, network-integrated PBX.

Traditional PBX systems can also be fully extended with Windows 2000 Server and TAPI 3.0. Authentication, security, user policies and phone directories can all be integrated between the PBX and Windows 2000 Active Directory. By installing Windows 2000 Server on a card within the switch, the telephone switch can integrate with data networks and take advantage of the open programmable network infrastructure of Windows 2000 Server. For example, telephone switches can integrate network-based call control features without the complexity of an external call control server. User policies for telephone access could be integrated with Active Directory to unify control of telephone and data services. Finally, the switches can use the integrated media stream services of Windows NT Server 5.0 to simplify scalable voice services.

Voice-over-data is another capability of Windows 2000 Server telephony support. Integrated ITU H.323, QoS, and CoS features provide a solid foundation for interoperable voice-over-IP with the ability to reserve bandwidth and prioritize traffic to guarantee audio quality. These capabilities are used by Windows Media Services and Microsoft NetMeeting and they can be applied to third-party voice and telephony solutions.

Finally, the Windows 2000 Server integrated dialer application, which uses TAPI 3.0, ITU H.323, and the Information Locator Services, can deliver a unique desktop dialing solution. The dialer provides Windows-based telephone handset and call control for dialing, answering and forwarding when used with TAPI integrated phones or switches. The dialer can also be used to place voice-over-IP calls to any dialer-enabled system in the network, using a simple microphone and multimedia speaker system connected to the system running Windows 2000. Calls can be easily conducted, with other people in a company, whenever a user is logged into the network, including remote users over VPN and RAS connections. By adding an inexpensive video camera to the Windows 2000-based PC, users can add videophone functionality. The Information Locator Service can also be configured to arrange conference calls using the dialer. The dialer solution can be further extended with other H.323 compliant applications, such as Microsoft NetMeeting, to add additional functionality. Finally, standard calls through the Public Switched Telephone Network (PSTN) can also be added to the solution with a voice-over-IP to PSTN gateway.

Telephony Services Summary

For customers seeking to integrate their network operating system with their phone system, Solaris 7 represents an unrealistic choice. Telephony support or integration features are not present in the operating system at all. Where telephony is a priority, Windows NT Server 4.0 or Windows 2000 are the only feasible choices. Of the two, Windows 2000 Server is the better choice, as its implementation of the Telephony API (TAPI) is an entire generation newer than that present in Windows NT Server 4.0, offering a considerable amount of additional programming flexibility. Windows 2000 Server is also better equipped to serve telephony applications. It contains numerous networking enhancements, such as QoS or CoS, that are of considerable benefit to voice or TAPI-based applications. Finally, the addition of the integrated Dialer application and ITU H.323 electronic conferencing protocol support provide in-the-box applications to allow customers to get started developing and deploying their telephony solutions.

Quality of Service

When deploying enterprise applications, network reliability is paramount to deployment success. To help ensure network reliability, system administrators need the capability to control traffic prioritization and service levels in order to ensure that the most important customers and applications receive priority. The Internet Engineering Task Force (IETF) has developed two standards – one for RSVP quality of service (QoS) and another for diff-serve class of service (CoS). For the purpose of this review, each network operating system will be evaluated on its ability to provide a QoS implementation conforming to the standards set forth by the IETF.

Solaris 7 Implementation Details

Solaris 7 offers support for the RSVP QoS standard via the Solstice Bandwidth Reservation Protocol 1.0. The two primary components of this support are a user-level daemon that handles the requests from applications for reservations, and an API interface to the protocol. These components must be downloaded and installed separately from the operating system. Unlike the implementation of QoS in Windows 2000, applications must be linked to this API in order to take advantage of the QoS feature offered by the protocol.

Additionally, in Solaris Enterprise Server, Solaris Bandwidth Manager is included as a core component. Solaris Bandwidth Manager provides complete control over network services. Through this management tool, you can monitor and control the bandwidth allocation. Because you can control allocations to users and applications, you can make Class Of Service (CoS) distinctions. These CoS capabilities help ensure mission critical applications have the bandwidth they need.

Bandwidth Manager also provides logging features, which allow you to track statistics and usage of network bandwidth. QoS policies can be stored in and managed through Sun Directory Services.

Windows NT Server 4.0 Implementation Details

Windows NT Server 4.0 offers no QoS implementation of any kind. Some rudimentary features, such as bandwidth throttling, are available on an application-by-application basis, such as in Internet Information Server 4.0, but no complete solution is available.

Windows 2000 Server Implementation Details

Windows 2000 Server offers a complete QoS implementation conforming to the IETF proposed standards for RSVP QoS and diff-serve class of service (CoS).

RSVP QoS Service

The RSVP QoS service is a request/grant type service where client-requested reservations are either allowed or disallowed based on a centralized policy and network resource availability. RSVP QoS policies are stored in the Active Directory and used by the network to grant or deny requests from workstations for QoS reservations.

RSVP services primarily benefit applications requiring consistent bandwidth or response levels. For example, streaming media or voice-over-IP solutions benefit from reserved bandwidth and response time for clear media quality. This is especially important on low-bandwidth links, such as those often found on many WANs. For these applications, Windows 2000 Server will mark packets and negotiate signaling with RSVP capable routers, allowing administrators to allocate bandwidth and response time to guarantee broadcast quality.

Applications do not have to natively support RSVP services in order to request QoS reservations. Tools are provided in the resource kit to make reservation requests for bandwidth and/or response levels on behalf of the customer’s application, allowing administrators to implement QoS without application changes.

Diff-serve CoS Services

Diff-serve CoS services provides a priority-of-service implementation for mission-critical applications where reservations may not make sense due to the intermittent nature of the application’s communications. CoS services allow communications to be prioritized for appropriate processing via network queues. Systems administrators establish policy that can be configured on Windows 2000 Server-based hosts that will subsequently mark application packets for priority of service. Network switches and routers can then provide preferential service to those packets. For example, a policy could be set to establish a higher priority for an e-mail application over all other traffic on the network.

The Windows 2000 Server QoS and CoS implementations also feature a complete set of APIs to integrate applications with the operating system’s QoS implementation. All policies are stored and centrally managed through the Active Directory service.

Quality of Service Summary

Solaris Easy Access Server offers support for QoS, but not CoS. Only the high-end Solaris Enterprise Server product provides both QoS and CoS support. Microsoft Windows NT Server 4.0 offers no QoS features of any kind, making it a poor choice for customers needing to guarantee bandwidth and application availability.

For enterprise customers needing QoS, Windows 2000 Server is the clear full-featured choice. Windows 2000 Server offers a complete QoS implementation complying with the IETF standards for QoS and CoS to provide both guaranteed bandwidth and traffic prioritization.

Application Services

Section Summary

As organizations shift away from legacy systems to distributed computing, having integrated application architecture is becoming a priority for many information technology environments. Key features of such an infrastructure include:

- Robust operating system kernel.
- SMP scalability and support for large amounts of physical memory.
- Distributed component model on which to build applications.
- Message queuing services for asynchronous communications and application integration.
- Integrated data access for access relational databases and other types of data stores.
- Web application platform including a framework for extending applications to the Internet and strong integration with the underlying operating system services such as security.
- Thin-client solution.

Windows 2000 Server is the most comprehensive solution. It provides the best scalability and it has the most performance optimizations within its kernel. With the latest version of Clustering Services, including Network Load Balancing Service, it also provides the best availability solution. The addition of COM+ provides the best distributed component model, featuring many unmatched capabilities such as queued components, an in-memory database, and a loosely coupled event model. The most sophisticated message queuing services implementation is also included, featuring complete integration with Active Directory. Web Application Services support is superb – building on the already excellent solution in Windows NT 4.0. Web Application Services support includes additional process management, flow control, and error handling pieces. Finally, data access support and the latest version of Microsoft Terminal Services provide the most sophisticated database connectivity and thin client solution of the three products evaluated.

Windows NT Server 4.0 is a good middle-of-the-road solution. It features excellent scalability within the operating system kernel. Additionally, an excellent clustering and load balancing implementation is provided. The combination of COM and Microsoft Transaction Server provide an excellent foundation on which to build distributed applications. Finally, message queuing services, integrated database access, and the available Terminal Server Edition as a thin-client solution make it a good choice. Web Application Services infrastructure is superior to that of Solaris 7. It uses Active Server Pages (ASP) as a Web application framework to extend COM-based applications to the Web. Additionally, transaction processing, asynchronous message queuing, and a very sophisticated data access infrastructure are all in IIS 4.0 but are sorely lacking in the Easy Access Server / Sun Web Server implementation.

Solaris 7 provides excellent support in key areas necessary for an application server. With the ability to support up to 64 GB of memory (on SPARC hardware), and 64 SPARC CPUs in an SMP environment, Solaris 7 offers significant performance and system resources to applications hosted on Easy Access Server. Where it begins to break down is in its distributed component model. Support is minimal, providing none of the advanced performance and reliability features found in the Microsoft solutions. Additionally, it only supports Java as a language choice, limiting its attractiveness to customers who use other development languages. Web Application Services infrastructure is also decidedly dated. It offers none of the advanced, integrated capabilities in Microsoft's solutions such as message queuing or transactions. Thin client solutions are available in the form of Java terminals or even as AutoClient workstations. Traditional UNIX terminal services are also available.

Feature Table

Feature	Solaris 7	Windows NT Server 4.0	Windows 2000 Server
Core Application Services			
Memory Protection	■	■	■
Virtual Memory	■	■	■
Maximum Addressable Memory	64GB	4 GB	64GB
Intel PSE 36 Support	□	■	■
Process Scheduling	■	■	■
Job Objects	□	□	■
Kernel Integrated Java Virtual Machine	■	□	□
I_2O Support	■	□	■
SMP Support	64 CPUs	32 CPUs	32 CPUs
Scatter/Gather I/O	□	□	■
Spin Count	□	□	■
High Performance Sorting	□	□	■
Application Availability Features			
Fail-over Clustering	■	■	■
TCP/IP Clustering & Load Balancing Services	■	■	■
Rolling Upgrade Support	□	□	■
Recovery from Network Failure Support	■	□	■
Component Object Model Integration	□	□	■
Plug-and-Play Support for Clustering Hardware	□	□	■
Directory/Clustering Services Integration	□	□	■
Distributed Application Model Features			
COM/DCOM Support	□	■	■
CORBA/IIOP Support	□	□	□
Java Beans Support	□	□	□
Enterprise Java Beans (EJB) Support	□	□	□
Graphical Component Management	□	■	■
Automatic Transaction Support	□	■	■
Configurable Security	□	■	■
Database Connection Pooling	□	■	■
Application Thread Support	□	■	■
Component State Management	□	■	■
Process Isolation	■	■	■
Legacy Transaction Integration	□	■	■
In Memory Database	□	□	■
Component Eventing Model	□	□	■

Language Neutrality	□	■	■
C++ Language Support	□	■	■
Java Language Support	■	■	■
Visual Basic Language Support	□	■	■
Dynamic Component Load Balancing	□	□	■
Data Access			
ODBC Support	■	■	■
JDBC Support	■	■	■
OLE DB Support	□	■	■
Data Access API Set	□	■	■
Message Queuing Services			
Message Queuing Implementation Available	■	■	■
Component Support	□	■	■
Transaction Support	□	■	■
Single API Set	□	■	■
Reliable, Resilient Message Delivery	□	■	■
One Time, IN-Order Message Delivery	□	■	■
Hierarchical, Directory Service-based Architecture	□	□	■
Message Routing Services	□	■	■
Clustering Service Support	□	■	■
MAPI Integration	□	■	■
Security Integration	□	■	■
Integrated Encryption, Integrity, and Signature Support	□	■	■
Security Log Integration	□	■	■
Web Application Services			
CGI Support	■	■	■
ISAPI/NSAPI Support	■	■	■
Server-side Scripting	■	■	■
Visual Basic Server Scripting Support	□	■	■
JavaScript Server Scripting Support	■	■	■
Java Servlet Support	■	□	□
Component Services Integration	□	■	■
Script Debugger	■	■	■
XML Integration	□	□	■
Customized Error Handling	■	□	■
Included Server Components	□	■	■
Message Queuing Integration	Optional	■	■
Server Scriptlet Support	□	□	■
Terminal Services			

Thin Client Solution Available	■	■	■
Supports 16-bit Windows-based Clients	■	■	■
Supports 32-bit Windows-based Clients	■	■	■
Supports UNIX Clients	■	■	■
Supports Mac/OS Clients	■	■	■
Supports Terminal-based Clients	■	■	■
Supports 16-bit Windows-based Applications	□	■	■
Supports 32-bit Windows-based Applications	□	■	■
Supports Windows 2000-based Applications	□	□	■
Supports DFS	□	□	■
Administration Tools	■	■	■
Deployment Tools	■	■	■
Configurable Security and Encryption	■	■	■

Core Application Infrastructure Services

As the business world shifts from host-based computing to distributed computing, a robust operating system on which to host mission-critical line of business applications is essential. The core operating system infrastructure must provide a robust platform with high availability and scalability to take advantage of the latest developments in server hardware. Essential features for an enterprise-level application server platform include:

- **Memory management** including memory protection, virtual memory support, and support for the latest standards to address large amounts of physical memory such as the Intel Page Size Extension 36 or Compaq Alpha Very Large Memory standards.
- **Process scheduling** to allow mission-critical applications to receive CPU priority.
- **Symmetric Multiprocessor (SMP) Support** should be provided to support up to 32 CPUs, which is the current industry standard.
- **Availability features** including fail-over clustering and TCP/IP load balancing services.
- **High performance** optimized operating system kernel.

Solaris 7 Implementation Details

The Solaris 7 Operating System was designed to take full advantage of the 64-bit UltraSPARC processor architecture. Solaris for x86, unfortunately, does not take full advantage of all the available features of the Intel architecture, such as PSE36 support. It is a safe assumption that when the 64-bit Intel processors ship, Solaris will be available on that hardware platform.

Memory Management

- **Virtual Memory** support is incorporated into the memory management system in Solaris 7. This ensures the most cost-effective use of physical memory possible. Solaris swaps infrequently accessed code areas to the hard disk, freeing physical memory space for caching and for more active code segments. This allows applications to address a memory space that is larger than the physical RAM in the server. Virtual memory is implemented transparently to the user and developer and grows and shrinks dynamically within the space allocated by the server administrator.
- **Addressable Memory** support in Solaris 7 has been enhanced, allowing it to directly address up to 64GB of

physical RAM. However, no support has been added to the x86 version of Solaris 7 to take advantage of the additional memory on Intel Xeon processors through PSE36.

Process Scheduling

The administrator is allowed to specify the amount of system resources, such as processor time, available to each application, and to prioritize them. This permits tuning for optimum responsiveness for critical applications that are competing for processor resources. Processor affinity is also supported.

SMP Support

SMP support in Solaris on UltraSPARC is capable of handling up to 64 processors. Support for Solaris 7 on x86 is limited to 32-processor hardware.

Availability Features

High-availability features such as clustering and load balancing are supported in the Solaris Enterprise Server extensions. They are not available in the entry-level Solaris 7 product. Other availability features include dynamic reconfiguration, hot-plug swap, and online upgrade capabilities.

Dynamic reconfiguration allows systems to continue running when system boards fail. System boards can then be replaced while the system is running.

Hot-plug swap enables administrators to add or remove subsystems and cards while the system is running. This capability provides strong management and control features for reconfiguring operational systems.

Online upgrade makes it possible to upgrade the operating system while the system is running. During the upgrade, the server remains operational and a reboot is not required.

Solaris Enterprise Server supports 4-node clusters and load balancing. For cluster management, Solaris Enterprise Server uses the Sun Cluster software. Sun Cluster provides an extensive GUI tool for ensuring the reliability, availability and serviceability of servers. For load balancing, Solaris Enterprise Server uses Solaris Resource Manager. Resource Manager can dynamically allocate unused resource capacity to improve application performance. Resource policies configured through the management tool also make it possible to rigidly control resource usage. Sun Cluster and Resource Manager are also available as separate products.

Java VM / OS Kernel Integration

Finally, Java Virtual Machine support is built directly into the Solaris 7 kernel. This provides a native ability to run Java applications on the Solaris 7 operating system platform. The Solaris Java VM provides complete compliance with all of the JDK 1.1 application programming interfaces (APIs) and supports Java database connectivity (JDBC), Java Naming and Directory Interface (JNDI), extended RMI functionality, and just-in-time (JIT) compilers. Excellent performance is available for Java applications and the easy ability to recompile the Solaris kernel removes most of the objections to necessity of making kernel changes when the Java standard is updated.

Windows NT Server 4.0 Implementation Details

Windows NT Server 4.0 was designed from the outset to be a robust, scalable platform for application services. To accomplish this design goal, an extremely sophisticated infrastructure has been developed to provide multiprocessor, advanced memory management, availability, and load balancing services within the Windows NT operating system.

Memory Management

Windows NT Server has provided advanced memory management features since its initial release. These include memory protection and support for virtual memory. With the release of Windows NT Server 4.0 Enterprise Edition, the addition of 3GB tuning was added.

3GB Tuning – Windows NT Server 4.0 Enterprise Edition presents an enhanced memory management implementation over that in prior versions of Windows NT. The standard edition of Windows NT Server 4.0 and prior versions provide a virtual 2-GB address space to every application. An additional 2 GB (for a 4-GB total between system and applications) is reserved by the operating system itself. Windows NT Server 4.0 Enterprise Edition extends this capability by allowing large memory-aware applications to use up to 3 GB, reserving only 1 GB for the operating system.

Addressable Memory – Windows NT Server 4.0 Enterprise systems running on Compaq Alpha processors can also take advantage of the underlying 64-bit architecture of the Alpha CPU. For example, Oracle Very Large Memory (VLM) for Windows NT Server on Alpha allows applications to benefit from the memory addressing capabilities of today's 64-bit Alpha processors. With VLM, Oracle can use up to 8 GB of physical memory in the Compaq AlphaServer 4100 and up to 28 GB of physical memory in the AlphaServer 8200 and 8400. Additionally, on Intel Pentium II Xeon based server systems with the Intel PSE 36 driver and a supported chipset, Windows NT Server 4.0 Enterprise Edition can access 36 GB of RAM for its applications.

Process Scheduling

Windows NT Server 4.0 provides minimal process scheduling support by allowing various applications and services to be assigned CPU priorities by the user. Additionally, at the highest level, two performance configuration options can be set to optimize the operating system as a whole for either workstation (foreground application services) or server (background application services) applications.

Multiprocessor Support

Windows NT Server provides support for machines conforming to the Symmetric multiprocessor (SMP) standard for multiple CPUs. It supports multiple CPUs on both the Intel x86 and Compaq Alpha processor families. In Windows NT Server 4.0 Enterprise Edition, 8 CPUs are supported out-of-the-box. Up to 32 CPUs are supported in custom configurations available from leading hardware OEMs.

Availability Features

Microsoft Clustering services ship as a standard feature with Windows NT Server 4.0 Enterprise Edition to provide clustering system services to guarantee high levels of application and data availability. Microsoft Cluster Server allows two servers to be connected into a cluster for higher availability and easier manageability of server resources. The two servers do not have to be the same size or configuration.

Microsoft Clustering services monitor the health of standard applications and servers, and automatically recover mission-critical data and applications from many common types of failure, usually in under a minute. Alternatively, system administrators can use the cluster service administration console to move workloads around within the cluster to balance processing loads or to unload servers for planned maintenance or testing without taking important data and applications offline for any significant period of time.

Out of the box, Microsoft Clustering server can provide high availability for most popular Windows NT services including file shares, print queues, Internet Information Server, Microsoft Transaction Server, and Microsoft Message Queue Server. Other popular applications supported by Microsoft Clustering server include Microsoft SQL Server™ 6.5 Enterprise Edition, Microsoft Exchange Server 5.5, and many popular products from Computer Associates, Cheyenne, Baan, Hewlett Packard, IBM, NetIQ, Octopus, SAP, and Vinca.

Network Load Balancing Service (NLBS) was recently introduced as a free upgrade to customers of Windows NT Server 4.0 Enterprise Edition. Microsoft Cluster Server is primarily aimed at providing availability for back-end applications and data services processing for such applications as Microsoft SQL Server. NLBS compliments Microsoft Cluster Server by providing availability and load balancing services to the front-end layer.

NLBS installs as a standard Windows NT network driver. Once installed, it operates in a transparent manner both to the TCP/IP server applications, such as Internet Information Server, and to TCP/IP clients on the network. Clients can access a NLBS cluster, which scales up to 32 nodes, via a single IP address. Under normal operations, NLBS automatically balances the networking traffic between the clustered computers, scaling the performance of one server to the level required by the administrator. When a computer fails or goes offline, NLBS automatically reconfigures the cluster to direct the client connections to the remaining computers. The offline system can then transparently rejoin the cluster and regain its share of the workload when it returns to service.

Windows 2000 Server Implementation

Windows 2000 Server uses the core application services infrastructure in Windows NT Server 4.0 as the basis of its core operating system implementation. Numerous improvements have pushed Windows 2000 Server to the leading edge in terms of scalability and availability.

Memory Management Improvements

The memory management infrastructure of Windows 2000 Server is greatly improved with the introduction of the Enterprise Memory Architecture (EMA). EMA allows Windows 2000 Advanced Server to take advantage of physical memories larger than 4 GB. Applications that are “large memory aware” can use addresses above 4GB to cache data in memory, resulting in extremely high performance.

Intel Pentium III Xeon microprocessors feature their own standards to take advantage of large physical memory arrays. Windows 2000 Server supports the Compaq Alpha Very Large Memory (VLM) and Intel Page Size Extension (PSE36). Windows 2000 Advanced Server machines can address as much as 64 GB of physical memory.

Multiprocessing Improvements

Windows 2000 Advanced Server continues to support 8 CPUs in the standard retail kit and 32 CPUs under the OEM terms and conditions of sale. This level of SMP support is unchanged from that of Windows NT Server 4.0 Enterprise Edition, but features a highly superior implementation of the SMP cod. This allows for better linearity of scaling on high performance. Performance will be most improved on systems with 8 CPUs or more.

Performance Optimizations

More performance optimizations have been made in Windows 2000 Server to improve CPU, memory, and I/O performance including:

- **New Winsock driver** (AFD) that provides the capability to complete large TransmitFile operations in an APC of the transmitting thread rather than posting it to a delayed system worker thread.
- **Enhanced memory allocation** – the per-processor look-aside lists reduce shared memory access of global look-aside list headers leading to a speedup of five percent for disk I/O.
- **Additional non-paged and paged pool lists** reduce pool fragmentation.
- **Reduced hold time** for the dispatch lock on workloads such as the TPC-C (such as Microsoft SQL Server 7.0 with fibers) reduces contention on key system resources by up to 30 percent.

- **Fibers** in Microsoft SQL Server 7.0 reduce context switches and improve throughput by up to 18 percent compared with threads.
- **Increased maximum working set for the file system cache** from 512 MB in Windows NT Server 4.0 to 960 MB in Windows 2000 Server. This reduces contention on system resources, thereby reducing context switching. On a SpecWeb ’96 workload, this improves throughput by up to 5 percent.
- **Per-processor completion ports** reduces CPU migration of threads, which provides a 5 percent to 7 percent increase in TPC-C throughput with Microsoft SQL Server 6.5.
- **NTFS improvements** reduce the number of operations posted to system worker threads, reducing context switching and thread CPU migrations by 46 percent and improving dual processor throughput on NetBench 5.0 by up to 3 percent.
- **Increased use of shared locks** for NTFS TransactionTable executive resource reduces contention on this resource by up to 14 percent for a multi-processor file-server workload.
- **Reduced SCSI miniport controller contention** (by a magnitude of seven) on Windows 2000 Server compared to Windows NT Server 4.0 on a TPC-C workload with Microsoft SQL Server 7.0.
- **Interrupt affinity** provides an improvement of up to 7 percent on a SpecWeb ’96 workload on a four-processor system using four NICs.
- **Reduction of TCP/IP contention** is expected to improve four-processor SpecWeb ’96 scaling by up to 20 percent.
- **Support for I2O hardware** has been added. With I2O, several significant performance enhancing benefits can be achieved. The most significant is the offloading of certain I/O operations to intelligent storage adapters, resulting in more available CPU cycles to process complex calculations and lower overall CPU usage.

Other Core Enhancements

Additionally, many enhancements to the applications server infrastructure have been made in Windows 2000 Server including:

- **Job Objects** are new kernel objects that can be named and secured. They are used to collect a group of related processes, enabling management and tracking of the process group. The Job Object enforces job quotas and security context. This enables the monitoring and control of per-process CPU time, per-job CPU time, minimum and maximum working set (memory usage), active process count, CPU affinity (which CPUs in a multi-processor system can run the processes) and priority class.
- **Scatter/Gather I/O** support enables higher I/O throughput when application data is located in non-contiguous memory locations (which is typical) and data needs to be written to a contiguous file location. It is VLM-enabled on the Alpha platform in Windows 2000 Server. The WriteFileGather API takes pointers to one or more pages in memory, gathers them together, and writes them out to the file as one chunk. ReadFileScatter reads in one or more pages from the file system and scatters them to pre-established buffers. The advantage of this technique is that the program need not work with intermediate buffers that contain the data as a single logical chunk.
- **Spin Count** is a new feature introduced to deal with the bottlenecks created by a specific memory block or resource that is constantly being acquired or released by a particular process. Usually a critical section guards these resources. However, if a thread blocks on a critical section, it is calling WaitForSingleObject(), which is relatively expensive. If the critical section for a resource is usually acquired and released in a fairly

short time period, the critical section can be optimized so that threads will not spend as much time in an expensive WaitForSingleObject() call. The dwReserved field of a critical section is now used for a spin count. If the spin count is set, a thread that would normally block while waiting for a critical section will instead enter a loop, where it continually checks to see if the critical section can be acquired. If the loop executes “spin count” a number of times, the thread gives up and reverts back to the old behavior by calling WaitForSingleObject(). The goal is that the blocking processor should acquire the critical section faster by this method than by using WaitForSingleObject(). It should be noted that spin counts do not result in any performance gain on single processor systems, but that the APIs can be called with no ill effects.

- **High Performance Sorting** support has been introduced in Windows 2000 Advanced Server. Specifically, commercial sorting performance of large data sets have been optimized, improving the performance of common tasks such as preparing to load data in batch for data warehouse/data mart operations and to prepare large sort-sensitive print and batch operations.

Availability Improvements

The Microsoft Cluster Server implementation in Windows NT Server 4.0 Enterprise Edition and the Windows Load Balancing Service have been enhanced and made standard features as part of the Windows 2000 Advanced Server package. Improvements can be summarized as follows:

- **Rolling Upgrades** allow administrators to easily take a server that is a cluster member offline for maintenance, permitting ”rolling upgrades” of system and application software. There are two major advantages to a rolling upgrade. First, service outages are very short during the upgrade process. Second, the cluster configuration does not have to be recreated – the configuration will remain intact during the upgrade process.

- **Active Directory and MMC Integration** has been added to the Clustering Service for Windows 2000 Advanced Server. The Active Directory service is automatically used to publish information about clusters. All management is now accomplished with the MMC, making setup easier and allowing administrators to visually monitor the status of all resources in the cluster.

- **Recovery from Network Failure** support has been added to the Clustering Service in Windows 2000 Advanced Server. A sophisticated algorithm has been included to detect and isolate network failures and improve failure recovery actions. It can detect a number of different states for network failures and then use the appropriate failover policy to determine whether or not to failover the resource group.

- **Plug and Play Support** can now be used by the Clustering Service to automatically detect the addition and removal of network adapters, TCP/IP network stacks, and shared physical disks, expediting configuration.

- **WINS, DFS, and DHCP Support** has been added to the clustering service for automatic failover and recovery. A File Share resource can now serve as a Distributed File System (DFS) root or it can share its folder subdirectories for efficient management of large numbers of related file shares. This provides a highly increased level of availability for mission-critical network services over prior versions of Windows NT.

- **COM Support for the Cluster API** has been added, providing a standard, cross-platform API set for developing and supporting cluster-aware applications. This API can be used to create scalable, cluster-capable applications that can automatically balance loads across multiple servers within the cluster. Additionally, the Windows Script Host (WSH) can control cluster behavior and automate many cluster administration tasks.

Core Application Infrastructure Services Summary

Windows 2000 Server provides a solid foundation architecture for building and running server-based applications. It provides customers with clustering services, resulting in higher application availability. Windows 2000 Server offers support integrated into the operating system for the Compaq Alpha Very Large Memory (VLM) and Intel Page Size Extension (PSE36) standards for addressing extremely large amounts of physical memory. Additionally, Windows 2000 Server provides support for I_2O, increasing the performance of disk-intensive applications on I_2O-capable systems. Finally, Windows 2000 Server provides mature integrated kernel optimizations such as SMP, memory protection and process management to increase the performance and robustness of enterprise applications.

Windows NT Server 4.0 provides customers with a solid foundation for running server-based applications. It suffers in comparison to Windows 2000 Server by lacking native support for the Intel PSE36 standard. Its clustering services implementation is an entire generation behind that of Windows 2000 Server and does not contain all of the numerous enhancements present in the Windows 2000 Server implementation.

Solaris 7 provides an excellent foundation on which to build server-based applications. On SPARC hardware Solaris 7 provides support for directly addressing 64 GB of physical memory (only 4 GB for Solaris on x86). As a 64-bit operating system (32-bit on x86) Solaris 7 provides a foundation for highly scalable high-performance application servers.

Distributed Applications Model

With the growing use of the Internet, organizations are looking at developing and deploying applications that run in a Web environment. Web applications are inherently n-tier, or distributed. An n-tier application separates the application into three distinct components:

- **Presentation** – The piece of the application that a user interacts with.
- **Application Logic** – The piece of the application containing all of the business rules and logic associated with the application.
- **Data** – The mechanism that stores and manages the data associated with the application, which is usually a relational database.

The benefits of authoring to a three-tiered model are many. Partitioning applications cleanly into presentation, business logic, and data layers enhances scalability, reusability, security, and manageability. Designers of distributed applications need to be able to deploy and reuse objects anywhere in a network without sacrificing security, scalability, or manageability. To this end, three standards have emerged as the basis for providing distributed component models – the Component Object Model (COM), the Common Object Request Broker Architecture (CORBA), and Enterprise JavaBeans (EJB).

To meet the challenges of today's application developers, a network operating system must provide a robust, integrated, distributed component model conforming to at least one of the three major standards. Distributed component object model implementations should meet the following technical requirements:

- **Language Independence** – Allows developers to author components in all popular programming languages.
- **Binary Standard Adherence** – Guarantees compatibility with other implementations of the same object model.
- **Component Services** – Provides a complete component object model on which component-based distributed applications can be built. Key features include transaction services to ensure data reliability, and a component manager, in which parameters such as security identification and process isolation can be configured.

Solaris 7 Implementation Details

The Solaris 7 distributed application model is based on CORBA/IIOP, Java Beans and the Enterprise Java Beans technology. The CORBA architecture is designed to allow platform-independent interoperability between objects in a distributed network environment. In this open environment, objects can discover each other and invoke services on each other via an Object Request Broker (ORB), regardless of location, implementation language, or platform.

The APIs and underlying communications protocol supported by the ORB conform to the CORBA and Internet Inter-ORB Protocol (IIOP). Therefore, ORB-based applications are portable and can interoperate with other CORBA-conforming implementations in heterogeneous network environments. Theoretically, this functionality and interoperability will work properly when communicating between CORBA/IIOP implementations.

CORBA-applications written on the Solaris 7 platform can fully interface with other CORBA applications running on other platforms and written in other languages via CORBA's IIOP protocol. CORBA applications on Solaris 7 are developed entirely in Java using the Interface Definition Language (IDL) as defined in the official OMG CORBA specification. Unfortunately, while Java language and IDL support is provided, Solaris 7 doesn't include an ORB and it doesn't include Java Beans or Enterprise Java Beans technology. This means you must purchase and/or install these components before you can create distributed applications on Solaris 7.

Windows NT Server 4.0 Implementation Details

Windows NT Server 4.0 ships with a complete, operating system-integrated implementation of the Component Object Model (COM). Introduced in the Windows operating system in 1993, COM is one of the most mature foundations for component-based applications. The key principles of COM can be summarized as follows:

- **Location Transparent** – Every COM component can be called with a process, across processes on a single computer, or across multiple computers without being recompiled.
- **Language-neutral** – Any popular language can be used to author COM components. On the Windows platform, support extends to Visual Basic®, C++, and Java. Developers authoring solutions in one language can easily use components written in other languages.
- **Discoverable Interfaces (DI)** – DI provides tools and other applications to discover the interfaces and parameters that are supported by the component, making it easy for developers to understand how to work with enterprise applications.

Distributed COM (DCOM), introduced in 1996, makes it possible to create networked applications built from components. With DCOM, developers can easily call and interoperate with components and applications running on other COM-capable systems over a network.

Beyond providing core support within the operating system, Windows NT Server 4.0 also provides an enhanced set of services for COM applications and developers. These services are included as the Microsoft Transaction Server (MTS) 2.0 in the Windows NT Option Pack. In a nutshell, MTS integrates COM components with transactions, providing a robust solution for developing enterprise-level, COM-derived applications. It also provides many important infrastructure pieces including the ability to graphically manage components and configure such settings as component security identification and process isolation. It is one of the most complete infrastructures available today on which to build distributed, component-based applications.

Functionality and benefits provided by MTS can be summarized as follows:

- **Automatic Transactions** allow configuring a component's transactional requirements when a component is deployed. The result is greater reliability and the potential reuse of business objects built as MTS components.
- **Configurable Security** allows a system administrator to define roles, then specify which interfaces and

components can be accessed by clients in each role, greatly simplifying the work required to create secure server applications.

- **Database Connection Pooling** allows components to reuse existing connections to a database rather than recreating new ones, simultaneously improving performance and scalability.
- **Automatic Thread Support** allows developers to write single-threaded components and then let MTS assign threads to those components as needed.
- **Component State Management** provides the Shared Property Manager (SPM) to allow components to store and then later retrieve their in-memory state after a component has given up its memory state at the end of a transaction. This provides greater flexibility in the types of COM applications that can be produced.
- **Process Isolation** allows individual COM applications to be grouped into one or more packages. Each package can then be run in its own process. This allows greater fault tolerance since the failure of a single component will only bring down the package of which the component is a member.

Windows 2000 Server Implementation Details

Windows 2000 Server enhances the COM and MTS implementation in Windows NT Server 4.0. It introduces COM+, an evolution of the technologies in Windows NT Server 4.0 and MTS 2.0. New features and benefits can be summarized as follows:

- **In Memory Database (IMDB)** provides an application with fast access to data, without incurring the overhead with storing and accessing durable state to and from physical disk. This allows frequently used data to be cached in memory and it provides a means for high-speed, low-overhead access, increasing the performance of data-driven COM applications.
- **Queued Components (QC)** allow clients to invoke methods on COM components using an asynchronous model. This provides many benefits to developers authoring applications intended to run on unreliable networks and in disconnected usage scenarios.
- **Dynamic Load Balancing** automatically spreads client requests across multiple equivalent COM components. This allows load to be distributed between multiple systems, increasing performance and scalability of COM applications.
- **COM+ Events** provides a publish-and-subscribe event service. Via a general event mechanism, multiple clients can “subscribe” to various “published” events. When the publishing application fires an event, the COM+ Events system iterates through the subscription database and notifies all subscribers. This allows more code reuse and lowers development costs. Programmers do not need to constantly modify code to take action when certain criteria (events) are met.
- **MTS Integration** has been implemented to fully tie together enhanced functionality in MTS with the core component services infrastructure in the operating system. Several improvements in functionality include broader support for attribute-based programming and integration with other transaction environments with support for the Transaction Internet Protocol (TIP).

Distributed Applications Model Summary

Windows 2000 Server is a strong choice for customers to build and deploy distributed component-based applications. The advanced features in COM+ -- Dynamic Load balancing, Queued Components, COM+ Events, and In-Memory Database -- provide unmatched ease of development, performance, flexibility, and scalability. on

Windows NT Server 4.0 is second only to Windows 2000 Server. It lacks equivalent functionality to the COM+ support. But the combination of COM as the distributed component model and Microsoft Transaction Server 2.0 provides a potent platform on which to develop enterprise applications. It has key benefits such as automatic transaction support, configurable security, database connection pooling, automatic thread support, state management, process isolation, and legacy host integration. These provide many essential features for developing component-based line-of-business applications that are simply not found in Solaris 7. In addition, it provides complete language neutrality, allowing developers to use their language of preference to deploy COM-based applications. This is in stark contrast to the Java-only CORBA implementation in Solaris 7.

Solaris 7 provides only limited support for the distributed application model through its support of Java and IDL. To create distributed applications, key components must be installed. A third party ORB is needed to handle requests between distributed objects. Java Beans or Enterprise Java Beans technology must also be installed to complete the distributed architecture.

Data Access

Most enterprise-level electronic line-of-business applications require some sort of database access in order to provide complete functionality. Integrated database access is an area that customers need to consider when choosing a networking operating system. Choosing an operating system without sufficient infrastructure to access corporate data has potentially time-consuming and costly ramifications. Review criteria for data access infrastructure include the following:

- Support for the industry-standard Open Database Connectivity (ODBC) standard.
- Native data access to popular databases such as Microsoft Access, SQL Server, and Oracle.
- An easy-to-use, extensible data access application programming interface (API) that is database provider independent and integrates with the operating system’s distributed component model and other application services.

Solaris 7 Implementation Details

Solaris 7 provides database access via support for ODBC and the Java Database Connectivity (JDBC) standards. ODBC support is incorporated into the Sun WebServer 2.1 to allow Web-based database access. JDBC is supported for any Java application running on the Solaris 7 server platform. No native database access is implemented within the operating system – all data access must be filtered through the ODBC/JDBC layers.

Windows NT Server 4.0 and Windows 2000 Server Implementation Details

Both Windows NT Server 4.0, with the Windows NT Option Pack, and Windows 2000 Server feature Microsoft Data Access Components (MDAC). Data driven applications can use the MDAC to easily integrate information from a variety of sources, both relational (SQL) and non-relational. MDAC includes the Microsoft ActiveX Data Objects (ADO), OLE DB, and Open Database Connectivity (ODBC).

ADO Implementation Details

ADO is the strategic application-programming interface (API) to data and information on the Windows platform. It provides consistent access to data and supports a variety of development needs, including the creation of front-end database clients and middle-tier business objects that use applications, tools, languages, or Internet browsers. ADO is designed to be the one data interface needed for single and multi-tier client/server and Web-based data-driven solution development. The primary benefits of ADO are ease-of-use, high speed, low memory overhead, and a small disk footprint.

ADO provides an easy-to-use interface to OLE DB, which provides the underlying access to data. It is optimized to provide minimal network traffic in key scenarios and it features a minimal number of layers between the front end and data source. It uses the familiar COM automation interface, available from all leading Rapid Application Development (RAD) tools on the market today.

OLE DB Implementation Details

OLE DB is Microsoft's strategic system-level programming interface to data across the organization. OLE DB is an open specification designed to build on the success of ODBC by providing an open standard for accessing all kinds of data. Whereas ODBC was created to access relational databases, OLE DB was designed for both relational and non-relational information sources, such as mainframe ISAM/VSAM and hierarchical databases; e-mail and file system stores; text, graphical, and geographical data; custom business objects, and more.

OLE DB defines a collection of COM interfaces that encapsulate various database management system services. These interfaces enable the creation of software components that implement such services. OLE DB components consist of data providers, which contain and expose data, data consumers, which use data, and service components, which process and transport data (such as query processors and cursor engines). OLE DB interfaces are designed to help components integrate smoothly so that OLE DB component vendors can bring high-quality OLE DB components to market quickly. In addition, OLE DB includes a bridge to ODBC to enable continued support for the broad range of ODBC relational database drivers available today. With Windows NT Server 4.0 and Windows 2000 Server, OLE DB providers for all popular databases are shipped standard as part of the operating system.

ODBC Implementation Details

The Microsoft Open Database Connectivity (ODBC) interface is a recognized industry standard and a component of the Microsoft Windows Open Services Architecture (WOSA). The ODBC interface makes it possible for applications to access data from a variety of database management systems (DBMS). ODBC permits maximum interoperability. For example, an application can access data in diverse DBMS through a single interface. Furthermore, that same application will be independent of any DBMS from which it accesses data. Users of the application can add software components called drivers, which create an interface between an application and a specific DBMS. With both Windows NT Server 4.0 and Windows 2000 Server, ODBC drivers are shipped with the operating system for connectivity to all popular databases.

Data Access Summary

For customers seeking to develop data enabled applications, Windows NT Server 4.0 and Windows 2000 Server are the most capable choices of the three systems evaluated. Full support for ODBC, the de-facto industry standard for data access, is provided along with operating system-integrated drivers for all popular databases. Additionally, Microsoft provides ADO – an easy-to-use, high-performance, COM-based API set for data access to virtually any provider - and OLE DB, a high-performance data access interface for most popular databases. With the advent of ADO and OLE DB, Microsoft is providing a comprehensive solution to address virtually any data access need for use against a variety of popular data providers – features that are simply unmatched by Solaris 7.

Solaris 7 data access choices are somewhat limited. ODBC support is provided for a small number of databases through Sun Web Server only. Additional ODBC drivers for the Solaris 7 platform must be acquired from third-party vendors, making database connectivity beyond the limited subset of supported databases a chore. Full support for JDBC is provided when connecting to a variety of databases.

Message Queuing Services

In virtually every industry, organizations are seeing an increasing need to enable their applications for network-based computing. The majority of the electronic application development solutions on the market today deal with the development of synchronous, real-time applications. However, in many organizations, there is also a significant need to build asynchronous, loosely coupled applications and reliable network communications services that will function properly over unreliable but cost-effective networks. A solution to this need is message queuing services. Features to look for in a network operating system message queuing implementation include:

- Integration with the network operating system's distributed component model.
- Simple application programming interfaces (APIs).
- One time, in-order message delivery.
- Transaction support with rollback.

Solaris 7 Implementation Details

Solaris 7 provides no message queuing services of any kind. Third-party solutions, such as the IBM MQSeries message queuing services, are supported.

Windows NT Server 4.0 and Windows 2000 Server Implementation Details

The Microsoft Message Queue Server (MSMQ) is integrated into the operating system in Windows 2000 Server and available as an add-on with the Windows NT 4.0 Option pack on Windows NT Server 4.0. MSMQ provides a complete, operating system integrated message queuing services implementation on the Windows platform. The core principles of MSMQ can be summarized as follows:

- All message queuing features and functions operate independently of network protocols. Any application that knows the name of another application's request queue can send requests and receive responses regardless of network type.
- Message queuing greatly reduces synchronization requirements between applications because message queue contents are easy to translate, and message-based interfaces hide the differences between application architectures and database technologies.
- To ensure reliability, message queuing sends data in a way that prevents message loss. In addition, the transactional delivery capabilities in message queuing make it easy to preserve data integrity within sending and receiving applications.

Through third-party solutions such as FalconMQ from Level 8 Systems, message queuing on the Windows platform can transparently access queues on legacy platforms managed by IBM Corporation's MQSeries product without requiring additional programming. When using message queuing to communicate to mainframe-based applications, as opposed to tightly coupled connections, the mainframe retains control over the order of request processing and database locking to optimize availability and performance.

Key features of the MSMQ implementation on the Windows platform can also be summarized as follows:

- **Full COM Component Support** has been provided with a set of integrated COM components that implement a convenient and full-featured application-programming interface to MSMQ features. COM support makes it easy to access MSMQ from a wide variety of popular programming languages such as Microsoft Visual Basic, Visual C++®, Visual J++®, and Microfocus COBOL as well as from Internet Information Server (IIS). This makes MSMQ one of the easiest to use and most accessible message queuing solutions available.
- **Simple Application Programming Interfaces** are provided to make development easier. The majority of

MSMQ programming is accomplished through five simple APIs (open, close, send, receive, and locate). MSMQ delivers its advanced message queuing benefits without complex network-level programming.

- **Reliable, Resilient Message Delivery** is accomplished through sophisticated techniques such as sliding window protocols, recoverable storage, and dynamic routing to deliver messages. This allows developers to focus on business logic and not on sophisticated communications programming.
- **One Time, In-Order Message Delivery** is guaranteed with MSMQ, ensuring that all messages are delivered exactly one-time and in the order that they were sent. This prevents many different kinds of problems that can occur within receiving applications such as duplicated orders and overdrawn accounts or inventories.
- **Transaction Support** is provided with full integration with Microsoft Transaction Server/COM+ and the Microsoft Distributed Transaction Coordinator (MSDTC). This provides a standards-compliant XA interface, enabling MSMQ operations to commit or abort with other resources in a transaction to preserve data integrity.
- **Hierarchical, Directory Service-based Architecture** has been implemented to manage all MSMQ objects dynamically. This improves scalability because administrative operations such as adding machines or moving queues can be performed centrally and do not require making changes to individual machine configurations. In addition, applications on any machine within an MSMQ enterprise can send messages to an application on any other machine with no pre-configuring of channels or routes. This dramatically improves scalability by eliminating management tasks that increase exponentially with the total number of connected machines. On the Windows 2000 Server platform, MSMQ is fully integrated with the Active Directory. All objects in an MSMQ enterprise can be managed as part of the directory just as if they were a standard directory object such as a user or group,. This greatly improves reliability and eases management-related tasks for the administrator.
- **Message Routing Services** are provided to deliver messages using the lowest-cost route that is currently available. When networks fail, MSMQ automatically uses the next-lowest-cost route to deliver messages. Administrators specify costs using the MSMQ Explorer. Routing support eliminates single points of failure and provides software-based fault-tolerance and high-availability.
- **Clustering Service Support** is fully provided with MSMQ. Clustering enables administrators using Microsoft Cluster Server on Windows NT 4.0 or Clustering Services on Windows 2000 to configure MSMQ services for automatic failover and fault-tolerant, high-availability applications.
- **MAPI/Microsoft Exchange Integration** allows MAPI transport provider services to use MSMQ as a communications medium. The MSMQ Exchange Connector enables MSMQ to send, receive, and transport Exchange messages and forms, making it easy for developers to add MAPI- and Exchange-based interfaces to MSMQ applications.
- **Security Integration** with the Windows NT and Windows 2000 Access Control List (ACL) mechanism. ACLs enable administrators to control precisely which users can perform read, write, and administration actions on a queue-by-queue basis.
- **Integrated Encryption, Integrity, and Signature** support has also been included with MSMQ. Message queuing applications can use the Microsoft Crypto API to automatically encrypt, protect, and sign messages. This protects messages from being viewed or changed during transmission (even over non-secure networks such as the Internet) and ensures that servers do not receive messages from unauthorized senders.
- **Security Log Integration** allows administrators to specify which MSMQ events (such as opening or closing a queue) should create an audit record in the Windows NT or Windows 2000 Security Log. This support

allows organizations to track the changes and events that affect their mission-critical applications.

Message Queuing Services Summary

For customers seeking to deploy message-queuing applications within their enterprises, Windows 2000 Server and Windows NT Server 4.0 are the only choices of the three operating systems evaluated. Both of the Microsoft solutions easily address all of the review criteria and provide many enhanced features and operating system integration benefits, making them both excellent solutions on which to deploy asynchronous applications. Of the two, Windows 2000 Server is the best choice because of the integration of MSMQ with Active Directory. With an integrated directory service that can track MSMQ objects, Windows 2000 provides the superior choice.

Web Application Services

In today’s e-commerce marketplace, where interactivity is one of the keys to success on the Internet, having developer-friendly, high-performance Web application services is vital to success. At minimum, a good Web application platform should include support for the following:

- Web application framework for extending applications to the Web.
- Server-side scripting model for easy application development.
- Support for transactions to guarantee data integrity.
- Database access infrastructure including native (non-ODBC) connectivity.
- Asynchronous message queuing services.
- Web application process isolation.
- Integration with the operating system’s distributed component model.

Solaris 7 Implementation Details

The Sun WebServer 2.1 component of the Solaris 7 package presents a Web development environment running on Solaris 7. Language support is available for Java, JavaScript, Perl, CGI, C, and C^{++}.

Scripting and Servlets

Native Web server scripting support is provided for JavaScript. Using the server-side JavaScript support built in to Sun WebServer 2.1, Web designers can build interactive server pages with JavaScript interpretation with execution occurring at the server. Via a CGI interface, scripts written in Perl can also be used via the Web server.

Java support is also available on the server. Developers can create Java servlets and access them from within pages being served by WebServer 2.1. Additionally, CGI scripts written in Perl or JavaScript can call and use Java servlets.

A key feature of Java servlets on Solaris 7 is that they are loaded, run, and administered dynamically, ensuring efficient use of server resources. Administrators can also administer servlets and make changes without requiring a server shutdown, maximizing availability. Because servlets are a server-side technology built into the operating system, they also have improved session management and better error recovery than client-based solutions.

Sun Network Cache Architecture

The most unique feature of Sun WebServer is the Sun Network Cache Architecture (SNCA). This technology allows static Web pages to be served at a rate unobtainable by any other Web server applications via a combination of caching and avoiding the TCP/IP protocol stack. The down side is that this performance improvement is limited to static content. Using SNCA with dynamic content can cause server crashes, and, in any case, shows little of the performance improvement that is available with static content, with Web performance being well below that of similarly configured Windows NT-based systems running Internet Information Server 4.0.

Management and Security

Installation and administration of Sun WebServer 2.1 can be handled through a browser-based administration tool or through command-line tools. The browser-based tool is quite powerful and allows administration of users, sites and servers. Through delegated administration, specific administration authority can be granted to administrators at local and remote facilities.

Windows NT Server 4.0 Implementation Details

IIS 4.0 integration with Windows NT Server offers an extremely rich development environment, supporting CGI, ISAPI, and Active Server Pages (ASP) technologies. As with most CGI implementations, any development language that is supported on the Windows NT platform can be used to build CGI scripts including all popular languages such as C, C++, Visual Basic, and Perl. ISAPI provides a standard API framework for extending the functionality of the Web server or developing advanced Web applications. Several other capabilities are also offered when using ISAPI over CGI. All aspects of IIS 4.0 can be managed through Microsoft Management Console.

Active Server Pages

Active Server Pages (ASP) product is Microsoft’s framework for building Web-based applications. With ASP, customers have the ability to quickly and easily develop and deploy interactive Web applications using script syntax that is as easy as that of HTML. Support for Visual Basic Scripting Edition (VBScript) and Jscript® are provided with the ASP implementation in IIS 4.0. Additional scripting language support can be provided via third-party script interpreters. Complex, interactive Web sites can be built quickly and easily with ASP at a significantly lower cost (in terms of required developer expertise, tools, and man-hours) than almost any comparable solution.

The ASP implementation in IIS 4.0 includes many reusable objects for commonly used tasks such as manipulating cookies, maintaining session state, implementing rotating banner advertisements, and accessing server and client information, such as user agent strings. One of the most important components is the Collaborative Data Objects (CDO) collection, which allows for integration with the IIS SMTP and NNTP services to easily build Web-enabled messaging applications with minimum programming knowledge and effort. Additional components are also available for such things as page hit counters from Microsoft’s Web site and many third party sources.

Data access is also fully integrated into IIS 4.0. Support for any ODBC- or OLE/DB-compatible data source is fully supported, providing for connectivity to all popular database systems. Microsoft ActiveX Data Objects (ADO) provide a standardized, easy-to-use, data-source independent API set. It is used for accessing and manipulating data from any ODBC or OLE/DB data source from any ActiveX-capable development platform, including ASP. Consequently, with the combination of ADO and ASP, building data-driven Web pages and applications is an extremely easy task that does not require much in terms of developer effort or expertise. This greatly reduces development and production costs when compared against comparable third-party solutions.

COM and MTS Integration

IIS 4.0 HTTP service also offers full COM integration with Microsoft Transaction Server (MTS) 2.0, which also ships as part of the Windows NT Option Pack. MTS 2.0 provides support for Transactional Active Server Pages. Transactional ASP allows for applications with scripts and components to perform multiple actions, with all actions committed together or none at all, providing mission-critical reliability for database-driven Web applications. Additionally, any COM-component can be used from within ASP scripts, and transactions support can be integrated between ASP scripts and COM components, providing an easy-to-use, robust infrastructure for developing multi-tier, scalable Web applications.

IIS 4.0 includes several other noteworthy application development features:

- **Microsoft Message Queue Server (MSMQ)** provides an easy way for applications to asynchronously send and receive messages over a network, ensuring reliable delivery even if part of the application or network becomes temporarily unavailable.
- **Script Debugging** support is integrated into IIS 4.0 to provide an integrated solution to debug ASP script applications, greatly easing development-related tasks.
- **Crash Protection (Isolated Process)** allows customers to run multiple Web applications reliably on the Web server. If one application crashes, the Web server and other applications will continue to run without interruption and the failed application will be automatically restarted on the next request. This provides for a considerably higher level of availability than in many competing solutions.
- **Java support** allows programmers to build server-side Java components and run them using the Microsoft Java 1.1 Virtual Machine. With the combination of Java components, Active Server Pages, and Transaction Server, Java developers can easily build enterprise-level Java-driven Web applications and run them efficiently in demanding server environments.

Windows 2000 Server Implementation Details

Windows 2000 Server uses the strong Web development foundation in IIS 4.0 as the basis of Internet Information Services 5.0. It adds several significant new features to produce a market-leading Internet applications platform. Key features in IIS 5.0 Web development support include:

- **Flow Control** features have been added to the IIS 5.0 ASP implementation. Now, rather than redirecting requests, Web developers can transfer requests directly to other pages on the server without incurring a round-trip to the client. This provides significant performance enhancements in applications where control is being transferred from one script to another.
- **Enhanced Error Handling** support allows developers to redirect server errors to customized ASP pages. With this feature, site administrators can display useful information such as the line number or description of where the error occurred. They can also execute special processing under certain conditions (such as electronically notifying administrators if certain fatal conditions are met).The enhanced error handling features also eliminate the need for developers to spend significant amounts of time writing custom error-handling procedures within their scripts and applications. This feature greatly reduces development time and expedites the deployment of sophisticated Web applications on the IIS 5.0 platform.
- **Server Scriptlets** support allows developers to encapsulate common scripts, such as those for database access or content generation, into reusable components accessible from any ASP script or COM-capable application on the IIS server machine. This gives developers easy-to-use scripting languages to create reusable components without a full-scale component development environment, such as Visual Basic, Java, or C++.
- **XML Support** is provided at the server, allowing developers to develop server-side XML-based applications

without requiring XML support on the client. This is an extremely important feature, as XML does represent the W3C's standard for data. Having support for XML at the Web server will be vital to interoperability with XML-derived systems as they become available.

- **Performance Enhancements** have been made in the Internet Information Services 5.0 implementation in Windows 2000 Server, especially on multi-processor systems for hosting out-of-process and ASP-derived Web applications.
- **COM+ Integration** in IIS 5.0 allows developers to take advantage of the new features in COM+ on Windows 2000 Server from within Active Server Pages, including IMDB, Queued Components, Dynamic Load Balancing, and COM+ Events. This provides a more flexible and powerful infrastructure on which to develop enterprise-level Web applications.

Management of IIS 5.0 is handled through the MMC.

Web Application Services Summary

Windows 2000 Server provides an integrated Web applications platform. With the ability to leverage integrated system services built into COM, customers can easily build powerful applications for the Web. Windows 2000 Server provides a number of features in addition to those found in Windows NT Server 4.0 including:

- Integration with platform services such as transactions, message queuing, security, and others.
- Server Scriptlets for better ASP scripting code reuse.
- Flow Control to reduce client-to-server round trips resulting in better performance.
- Enhanced Error Handling to make it easier for developers to handle exceptions.
- Process Isolation for Web-based applications to provide customers with a higher level of reliability.

Windows NT Server 4.0 Web server application services represent an excellent implementation that is second only to that in Windows 2000 Server. Along with Windows 2000 Server, it is the only offering to feature integrated message queuing, transaction processing, script debugging, and process isolation for maximum server reliability. Additionally, its data access infrastructure, server scripting language support, and collection of reusable components offer a more complete solution than that offered by Sun with the combination of Solaris 7 and Sun WebServer 2.1. Finally, due to the popularity of Active Server Pages, both the Windows NT Server 4.0 and Windows 2000 Server implementations benefit from a following in the developer and third party tools community. This makes support and enhancements easily obtainable; a significant advantage over the Solaris 7 Web application platform.

Sun bundles Sun WebServer 2.1 as part of Solaris 7, but provides little or no integration with other system services; thus making it difficult for customers to develop and deploy Web-based applications. Most language choices force the use of CGI-derived solutions and the associated negative implications. The Sun WebServer 2.1 server-side JavaScript implementation is the only native-server scripting solution, but its relative unpopularity in the marketplace makes it a somewhat proprietary and unsupported platform on which to develop Web applications.

Data access support is considerably behind either of the Microsoft solutions, making Sun WebServer 2.1 a poor choice for hosting data driven Web applications. There are simply no equivalents to most of the powerful application development features in the Microsoft solutions such as an integrated debugger, transaction support, or asynchronous queued message support. The only area in which Sun WebServer 2.1 excels over the Microsoft solutions is Java support. Java servlets are fully supported on the Solaris platform but are not present on either of the Microsoft solutions, making Sun WebServer 2.1 potentially a better choice in some respects for environments with large investments in Java technology. Apparently, not even Sun itself is willing to build heavily on Sun WebServer 2.1 as its own Web sites run primarily on various versions of Netscape Enterprise Server. The recent agreement with AOL over the division of the Netscape assets, in which Sun continues to build on the Netscape Web server platform, further clouds the future for the Sun WebServer application.

Terminal Services

Centralized administration and thin clients are issues of priority today for many IT departments in organizations around the world. The need for thin clients is being driven by the desire to lower device and management costs as well as adequately meet new application and user requirements, such as kiosk-type applications in a hotel room or airport.

Terminal Services offers the Windows experience on a diverse set of desktop hardware, providing a complete, Windows-based thin-client solution. It simultaneously provides all of the benefits of distributed computing and centralized administration, as in a mainframe model, to Windows customers. Specifically, Terminal Services delivers the Windows NT operating system experience to desktops that cannot currently run the 32-bit Windows operating system. Examples of such desktops include dedicated thin client devices, personal computers running 16-bit versions of the Windows operating system, Windows CE-based devices, or UNIX and Apple Macintosh based machines (available through an add-on package).

Terminal Services provides clients access to 32-bit Windows-based applications running entirely on the server. Multiple client sessions are supported at the server. The server manages all computing resources for each client connected to the server and provides all active users with their own operating environment. All keystrokes and mouse clicks sent by the remote client are received and processed by the server. All display output for both the operating system and applications are sent to the appropriate client. After logging on, users can access all of their authorized network resources and can run applications made available to them on the server. Because Terminal Services supports virtually every application supported by Windows NT, users potentially have access to virtually all major 16- and 32-bit Windows-based applications via a thin client environment.

Solaris 7 Implementation Details

If there is one area in which Solaris 7 shines it is in the availability of thin clients. The multi-user environment is where Solaris and other UNIX variants were originally developed. Therefore, it is no surprise that a wealth of tools and third-party applications can take advantage of the multi-user aspects of the server via various types of thin clients.

The most common thin client implementation is probably that of the X terminal. This is a device (specialized terminal, PC with appropriate software, etc.) that runs an X Windows application that allows it to remotely execute applications on the server with a local console session. This is a very mature technology and enjoys wide support from the vendor (both software and hardware) community.

Though not as popular, various Java-based solutions, ranging from Java-only terminals to Java applications running on a PC, offer the same type of support available from an X Windows terminal in running remote applications. They also add the ability to locally execute Java applications.

While not specifically a thin client solution, the Solstice AutoClient application allows systems to remotely boot from a Solaris 7 server. All system files and user data are stored on the server and only cached on the client machine while the session is active. These clients can run an X Windows session while maintaining the full processing power of the local workstation. They also give the system administrator the benefits of centralized administration available to the other thin client solutions. Therefore, it is a very popular alternative in the Solaris 7 environment. As of version 3.0, however Solstice AutoClient is no longer included with Easy Access Server. You must obtain and install this component separately from the operating system.

If there is a single weak spot in the thin client support available for Solaris 7, it is the lack of an integrated management solution for the thin clients.

Windows NT Server 4.0 Implementation Details

The Windows NT Server 4.0 Terminal Server Edition is a separate edition of Windows NT Server 4.0 with the Terminal Services feature integrated into the operating system.

The Terminal Services feature extends Windows NT Server 4.0 to provide true, multi-user support. The operating system has added two new management tools – Client Connection Manager and License Manager – to help administer Terminal Services. Client support is provided for 16-bit and 32-bit Windows-based machines. Additional client-support for Macintosh or UNIX-based clients is obtainable through Citrix MetaFrame. Windows-capable terminals, such as those available from Tektronix, NCD, Cruise Technologies, Boundless Technologies, Wyse, or Neoware connect to a machine running Windows NT Server 4.0 Terminal Server Edition as-is – no additional client software is required.

The Client Connection Manger utility, available as part of the Terminal Services Client software, allows administrators and end users to setup predefined connections to one or several servers for single application or full desktop access. It creates an icon that can be used for single-click connectivity to one or more Terminal Servers. This provides the necessary support for administrators to provide a single line-of-business application across an entire enterprise by simply creating an icon, saving it, and then distributing it using the client software to all desktops.

The License Manager tool assists system administrators and purchasing officers in keeping track of client connectivity for license monitoring and tracking purposes. It is similar to the licensing tools provided as part of Windows NT Server 4.0, except that it has been modified to track per desktop. Licensing continues to be honor-based as has always been the policy with Windows NT; the tool has been provided merely to aid administrators.

Application compatibility has been a focus for Terminal Services throughout the development process. Almost all applications that will run in a Windows NT 4.0 environment will run on Terminal Services. Microsoft has performed extensive testing on a wide range of applications and has provided setup scripts for all popular business and productivity applications to help address any multi-user issues that may arise.

Windows 2000 Server Implementation Details

Terminal Services have been fully integrated into the Windows 2000 Server as an optionally installable service and is no longer shipped as a separate product. Every feature in the Windows NT Server 4.0 Terminal Server Edition is present as part of the Terminal Services feature of Windows 2000 Server. However, the Terminal Services implementation in Windows 2000 Server has been enhanced to support Windows 2000-based applications and the new features in the Windows 2000 environment. This is in addition to continuing to provide full support for all existing 16- and 32-bit Windows-based applications.

Also new in Windows 2000 Server is Distributed File System (DFS) support. Terminal Services clients can connect to a DFS share and DFS shares can be hosted from machines running on Terminal Services. A new MMC based utility facilitates the creation and distribution of client software for Terminal Services. Additionally, several new features are under development for inclusion in the Windows 2000 Server edition of Terminal Services including an RDP Web Client (via an ActiveX control), load balancing, shadowing, public Terminal Services APIs, support for all OLE/DCOM activation modes, persistent caching, and redirection of COM, printing, clipboard, and audio.

Terminal Services Summary

Where thin client support is a priority, Windows NT Server 4.0 Terminal Server Edition and Windows 2000 Server provide a thin client solution that runs standard, line-of-business Windows-based applications such as Microsoft Office. In Windows 2000, terminal clients can connect to and host DFS shares.

Solaris 7 provides a wealth of thin client solutions. These solutions range from the traditional UNIX serial terminal-based connection option through Java clients. The most widely used thin client solution is X Terminal.

X Terminal is a very mature technology and enjoys wide support from the vendor community. Beyond a strict thin client solution, Solaris 7 also supports Solstice AutoClient. With AutoClient workstations, all operating system files and services are loaded from a server.

Internet Services

Section Summary

Web services infrastructure determines a network operating system's ability to publish information using Internet standards, and ability to interoperate with other systems while using standardized Internet protocols. A solid solution should include infrastructure to support:

- The latest Internet standards.
- Multi-site Web hosting.
- Strong Internet Security.
- Easy and flexible management.
- Comprehensive content management and log-file analysis.
- Features for added scalability and availability.
- Streaming media.

Windows 2000 Server builds on the integrated Internet services in Windows NT Server 4.0. Its Wizards and MMC Task Pads make it an easy solution to configure and administer on a daily basis. It is the only solution to offer advanced flow control, error handling, process accounting, CPU throttling, and support for WebDAV, making it clearly stand out from the competition. In other areas, Windows 2000 Server generally offers a more comprehensive or better performing solution than the other two operating systems.

Although Windows NT Server 4.0 does not offer the advanced features of Windows 2000 Server, it generally offers a good portion of the core functionality. Aside from Windows 2000 Server, IIS 4.0 on Windows NT Server 4.0 is the only solution to offer SMTP and NNTP services. Additionally, Microsoft Cluster Server and the Windows Load Balancing Service, present on both Windows NT Server 4.0 and Windows 2000 Server, provide fault-tolerance and load-balancing services.

Internet capabilities in Solaris 7 are provided through Sun WebServer 2.1, Solstice Internet Mail Server 2.0, a native FTP Server and a native Telnet server. However, the lack of integration with the core operating system and limited feature support result in a more complex solution than offered in the Microsoft solutions. Manageability is difficult, featuring separate, non-integrated tools for Internet services management. Sun WebServer 2.1 does not truly integrate with the operating system's security model, requiring an LDAP interface to Sun Directory Services (if it is actually being used) for security authentication. Core feature support is also not as good as that offered by Microsoft. Difficulties and limitations in configuring and managing multiple servers arise often.

Feature Table

Feature	Solaris 7	Windows NT Server 4.0	Windows 2000 Server
Internet Standards Support			
HTTP 1.1 Compliant	■	■	■
FTP	■	■	■
SMTP	■	■	■
IMAP4	■	□	□
POP3	■	□	□
NNTP	□	■	■
Telnet	■	□	■
MIME	■	□	□
WebDAV	□+	□	■
HTTP Compression	□	□	■
FTP Restart	■	□	■
Multi-Site Web Hosting			
Virtual Directories	■	■	■
Virtual Servers	■	■	■
Host Header Support	■	■	■
Centralized Administration	■	■	■
Unique Configuration for Each Server	■	■	■
Delegated Administration	□	■	■
Bandwidth Throttling	□	■	■
Process Accounting	■	□	■
CPU Throttling	■	□	■
Multiple User Domains	■	□	■
Internet Security			
Basic Authentication	■	■	■
Encrypted Authentication	■	■	■
X.509 Certificate Authentication	■	■	■
OS Integration for User Authentication	□	■	■
40-bit SSL Encryption	■	■	■
128-bit Strong SSL Encryption	■	■	■
TCP/IP Address Restrictions	■	■	■
DNS Domain Restrictions	■	■	■
Wizards and Tools for Automated Configuration	■	□	■
Digest Authentication	□	□	■

Internet Services Administration			
GUI-based Administration	■	■	■
Browser-based Administration	■	■	■
Command line-based Administration	■	■	■
Integrated Management Solution	■	■	■
API Set for Custom Management Scripts	□	■	■
Ease-of-Use Wizards	■	□	■
Content Management and Logging			
Redirection	■	■	■
Custom Error Pages	■	■	■
Custom HTTP Headers	□	■	■
Custom Footers	□	■	■
PICS Support	□	■	■
HTTP Content Expiration	■	■	■
Content Indexing	□	■	■
FrontPage Server Extensions	■	■	■
Internet Services Scalability and Availability			■
Load Balancing Service	■	■	■
Fail-over Clustering Service	■	■	■
Streaming Media Services			
Streaming Media Services Solution	□	■	■
Streaming Audio	□	■	■
Streaming Video	□	■	■
Low-bandwidth Audio Codecs	□	■	■
High-bandwidth Audio Codecs	□	■	■
Low-bandwidth Video Codecs	□	■	■
High-bandwidth Video Codecs	□	■	■
Integrated Security	□	■	■
QoS Solution Available	□	□	■

+Solaris 7 supports WebNFS, which is similar in some respects to WebDAV.

Internet Standards Support

Internet standards refer to the Internet protocol support provided by an Internet services implementation. A complete connectivity solution should provide, at minimum, support for all major Internet services protocols, including:

- Hypertext Transfer Protocol (HTTP).
- File Transfer Protocol (FTP).
- Simple Mail Transport Protocol (SMTP).
- Network News Transport Protocol (NNTP).

Additionally, many recent developments in Internet technology have resulted in the support of three enhancing protocols, all of which should be supported by an up-to-date Internet services implementation:

- WebDAV is the IETF's proposed extension to the HTTP 1.1 protocol to provide a Web-based protocol for file management and publishing.
- FTP Restart allows interrupted FTP transfers to be resumed without having to start from scratch.
- HTTP Compression caches and compresses static pages and provides on-the-fly compression of dynamic files to help reduce download time and improve performance for end-users.

Solaris 7 Implementation Details

Sun WebServer 2.1 and Solstice Internet Mail Server 1.0 are included with Solaris 7. Together with native FTP and Telnet servers, these products represent a complete Internet service offering that in some aspects exceeds the offering in Windows NT 4.0 and Windows 2000.

Sun WebServer 2.1 provides a solid HTTP service implementation and complete support for HTTP 1.1. WebServer 2.1 features an improved Web-based administration tool and administration wizards to help configure users, sites and servers. However, these tools aren't as easy to use as those in Windows NT 4.0 or Windows 2000. The HTTP service supports SSL encryption, Basic Authentication, access control lists at the file/directory level and domain-level restrictions. Domain-based virtual server hosting offers a flexible, scalable solution.

Solstice Internet Mail Server 1.0 offers the most complete mail service of the three network operating systems. This is a complete mail server solution, supporting SMTP IMAP4, POP3 and MIME. Messages can be sent securely using SSL encryption. Messages can also have email attachments. Solstice Internet Mail Server is also a completely scalable mail solution.

Native Telnet and FTP services are an important part of Solaris 7. With Telnet, users can connect to remote computers and execute commands at the command-line. With FTP, users can connect to remote computers to upload or download files. Solaris 7 supports both anonymous and user account-authenticated FTP services. User account authentication, along with file permissions, serves to control access to files and directories.

Solaris 7 provides support for WebNFS, which is a standard for accessing Web-based information. In some respects, WebNFS is similar to WebDAV. WebNFS was discussed previously under File Sharing and Storage Services. WebDAV is discussed later under Content Management.

Windows NT Server 4.0 Implementation Details

Included in the Windows NT Option Pack, available as an add-on for Windows NT Server 4.0, is Microsoft Internet Information Server (IIS) 4.0. IIS 4.0 is Microsoft's fourth-generation Internet services implementation and comes integrated with HTTP (Web), FTP, SMTP, and NNTP services. Details are as follows:

- **HTTP Service Implementation –** IIS 4.0 provides a comprehensive HTTP service offering more features than that found in the Sun WebServer 2.1 shipped with Solaris 7. Both the HTTP 1.0 and 1.1 protocols are supported, providing simultaneously for maximum compatibility and performance.
- **FTP Service Implementation –** With regard to the FTP service shipped with IIS 4.0, both anonymous and user account-authenticated FTP is fully supported. User account authentication, along with file permissions, is based on Windows NT Server 4.0 domain or local account databases, providing complete OS security model integration. Additionally, up to 255 virtual FTP servers, each maintaining its own configuration information can be created on each IIS server.
- **SMTP Service Implementation** – As mentioned previously, an SMTP service implementation is included

with IIS 4.0 for integration with Internet email solutions. Mail support for both local and remote domains is provided along with full SMTP relaying capabilities. A smart host feature is also included to allow for SMTP routing and forwarding to other Internet mail servers. The SMTP service also supports SSL encryption – both 40-bit standard and 128-bit strong encryption – allowing for the secure transmission of messages between clients and the IIS server.

- **NNTP Service Implementation** – An NNTP service implementation provides USENET news connectivity. With the NNTP service, a complete article expiration facility is provided to purge old messages. Integration with the SMTP service is also present to allow for moderated newsgroup postings, giving administrators control over the content posted to the server. As with the SMTP service, SSL encryption at both 40-bit standard and 128-bit strong encryption is supported, providing for secure transmission of information between clients and the IIS server. Access to the server can be restricted on a per account, TCP/IP address, or DNS domain basis in a manner similar to that featured on the other IIS services.

Windows 2000 Server Implementation Details

Windows 2000 Server provides a comprehensive and fully integrated Web service solution. IIS 5.0 includes all features and capabilities in the IIS 4.0 plus many enhancements.

The major enhancement to Windows 2000 Server in the area of Internet Standards is support for WebDAV (discussed below under content management) and the addition of Digest authentication (discussed below under Internet Security). Other improvements include:

- **HTTP Compression,** which provides integration of the industry-standard HTTP compression protocol. It compresses and caches static files and optionally dynamically generated files. This provides faster transmission of pages between the Web server and compression-enabled clients such as Microsoft Internet Explorer 4.0 and 5.0.

- **FTP Restart,** which allows the resumption of interrupted FTP file transfers between a client and an IIS 5.0 FTP server. This provides a smoother and less time consuming approach to all users downloading information from IIS 5.0.

Internet Standards Support Summary

Windows 2000 Server provides a comprehensive set of Internet standard protocols, including – HTTP 1.1 and FTP compliant services, HTTP Compression, FTP Restart, SMTP, NNTP, and especially the recently IETF-ratified WebDAV standard.

Shipped with the Windows NT Option Pack for Windows NT Server 4.0, Microsoft IIS 4.0 provides a complete Internet server solution. However, Windows 2000 Server provides additional standards such as HTTP Compression, FTP Restart, and WebDAV.

Solaris 7 Internet services implementation with Sun WebServer 2.1 and the native FTP Server provides support for all basic Internet standards with the exception of the recently proposed WebDAV. While the product does not include an NNTP server, Solaris 7's Solstice Internet Mail Server does support IMAP4, POP3 and MIME, which aren't supported by Windows NT 4.0 or Windows 2000.

Multi-Site Web Hosting

The ability to host multiple Web sites on a single server system represents a significant priority for many corporate customers and ISPs. By providing this capability, a considerable amount of resources can be saved by not using multiple servers, by reducing administration costs, and so forth. Things to look for in a multiple-site hosting solution are as follows:

- Ability to host multiple sites from a single software installation.
- Each site should have its own unique configuration but be centrally manageable.
- Host headers and multiple TCP/IP address hosting should be supported.
- Bandwidth throttling to ensure that all traffic can get through and that no site can overtax the Web server system.
- CPU throttling to ensure that no Web application can overcome the CPU, and that adequate processor time is available for all Web applications.

Solaris 7 Implementation Details

Through Sun WebServer 2.1, Solaris 7 supports a scalable virtual hosting service. Virtual hosting allows multiple sites to be hosted on a single server. Multiple sites are supported either via multiple TCP/IP addresses or host headers, allowing for multiple sites to be hosted on a machine with a single or limited number of TCP/IP addresses.

Sun WebServer 2.1 supports server-level and site-level administration as well as delegation of administration. Domain-based virtual hosting allows unique name spaces (user domains) to be assigned to each site on the server. Administration delegation and domain-based hosting are especially beneficial to ISPs hosting multiple sites. They can have separate account databases for each site, and each domain can be securely controlled by its own administrator.

Sun WebServer offers the ability to host multiple virtual Web sites (up to eight according to the documentation, 24 according to the information on the Sun WebServer website). Also, the Solaris 7 product license for Sun WebServer 2.1 allows the Web server software to be installed on up to four machines.

Windows NT Server 4.0 Implementation Details

Virtual Servers (multiple Web sites) are supported per machine, providing for maximum flexibility in environments where multiple site hosting is required. Multiple sites are supported either via multiple TCP/IP addresses or host headers, allowing for multiple sites to be hosted on a machine with a single or limited number of TCP/IP addresses.

In addition to support for virtual servers, Windows NT Server 4.0 provides a number of other features to enhance the multi-site hosting capabilities of the Web server. These include:

- **Web Site Operators** – Administrator can be assigned management privileges on an individual Web site basis. This allows organizations to host multiple Web sites on a single server, while keeping the administration of the individual Web sites separate.
- **Bandwidth Throttling** –Where bandwidth is limited, the server administrator can set the amount of bandwidth each site on a server with multiple sites can use.

Windows 2000 Server Implementation Details

Windows 2000 Server builds on the features in Windows NT Server 4.0 to provide an even stronger solution for hosting multiple Web sites on a single server. New features include:

- **Process Accounting,** which provides system administrators information about how Web sites use CPU resources on the server. This feature can be enabled and customized on a per-site basis. It provides many benefits to administrators, especially in multi-site environments. It can identify rogue scripts that are eating CPU cycles or malfunctioning processes, helping to ensure that processor time is available to other Web sites or applications.

- **CPU Throttling,** which uses the Job Object in Windows 2000 Server to allow administrators to limit the amount of CPU processing time a Web application or site can use over a period of time. CPU Throttling provides several benefits to users, especially those running multiple sites or applications on the same server. It limits the amount of time a Web site's applications are allowed to use the CPU, ensuring that processor time is available to other Web sites or non-Web applications.
- **Multiple User Domains,** which allow unique name spaces to be assigned to each site on the IIS server. This feature is especially beneficial to ISPs hosting multiple sites. It allows separate account databases for each site and allows each domain to be securely controlled by its own administrator.

Multi-Site Web Hosting Summary

Windows 2000 Server provides Process Accounting, which allows administrators to track CPU usage on a per-site basis, greatly easing management tasks. It also provides CPU Throttling, allowing CPU time to be limited on a per site or per application basis. Finally, the ability to have multiple user databases (domains) for each site makes it an excellent choice for Internet Service Providers.

Windows NT Server 4.0 provides a true multiple site hosting environment, multiple virtual servers each centrally manageable but with their own unique configurations. In conjunction with Windows 2000 Server, it is the only solution to provide bandwidth throttling and delegated administration capabilities.

Sun WebServer 2.1 offers the ability to host multiple virtual Web sites and to delegate administration. While these features are adequate for most needs, administrators will miss the throttling and process accounting functions of more full-featured Web servers, such as IIS 5.0.

Internet Security

Internet security is a major concern to any organization providing information and services over the Internet. It is critical that a Web server solution provide:

- **Authentication** – A way for clients using a Web browser to authenticate themselves to the Web server. The solution should include support for standard authentication protocols such as Basic and Digest Authentication for use over the Internet, and single sign on services for authentication in a trusted domain such as an intranet.
- **Encryption** – Support for standard Secure Sockets Layer (SSL) encryption in both standard (40-bit) and strong (128-bit) encryption strengths.
- **Access Control** – The ability to control which files users can access.
- **IP Security** – The ability to grant/deny access based on the IP address and/or domain of the end user.

Solaris 7 Implementation Details

The specifics of the Solaris 7 Internet security infrastructure are as follows:

- **Authentication** – Support for standard authentication features is fair. Both Basic Authentication and encrypted authentication are supported. Basic X.509 certificate-based authentication is also supported. Operating system integration for user account authentication is available through the */etc/password* and */etc/shadow* files, but direct integration in this manner is not recommended by Sun and may open the system to attacks or other serious security problems.
- **Encryption** – Support for Secure Sockets Layer (SSL) encryption is provided, for both 40-bit and 128–bit

Strong SSL encryption.

- **Access Control** – Access can be restricted on a per user basis either using the integrated account database or user accounts from an LDAP-compliant directory, such as Novell NDS or Microsoft Active Directory.
- **IP Security** – Sun WebServer 2.1 provides a comprehensive security implementation to restrict access to content. Access to content can be restricted on a per user, TCP/IP address, or DNS domain basis.

Windows NT Server 4.0 Implementation Details

The specifics of the Windows NT Server 4.0 Internet security infrastructure are as follows:

- **Authentication** – A comprehensive array of authentication options is provided with the Web services present in Windows NT Server 4.0. Support for both basic (non-encrypted) and NTLM (encrypted) password authentication is provided when authenticating against the Windows NT Server directory. Authentication is based on Windows NT Server 4.0 domain and local user account databases. This provides for complete, native integration with the Windows NT Server 4.0 security model and eliminates the need for account synchronization or separate user account databases. Additionally, X.509 client certificates can be mapped to Windows NT user accounts for security authentication using digital certificates.
- **Encryption** – Secure Sockets Layer (SSL) data encryption is fully integrated into IIS 4.0. Support for both 40-bit and 128-bit strong encryption provides complete encryption support for virtually any scenario. Server Gated Cryptography is also supported, for the strongest (128-bit) encryption possible for completely secure online transactions for customers such as international banks.
- **Access Control** – Since IIS is an integrated service, it leverages the security infrastructure built into Windows NT Server. Therefore access to files from Web browsers is controlled by adding a user to the Access Control List (ACL) for a file or group of files. This is the same procedure an administrator would follow to provide access to a file on a file server; thus eliminating the need for an administrator to learn a new security model.
- **IP Security** – Content can be restricted based on user accounts, TCP/IP addresses, DNS domain names, or any combination thereof.

Windows 2000 Server Implementation Details

The Windows 2000 Server security infrastructure adds a number of features to make it easier for administrators to secure their Web servers. These include:

- **Certificate Wizard** provides a tool to automate and ease the often-difficult task of setting up SSL-encrypted Internet services. The Certificate Wizard allows administrators to quickly and easily deploy encryption technologies without the difficult setup process in prior versions and products from the competition.
- **Permission Wizard** provides a tool to automate the tasks of configuring security permissions and authenticated access on IIS 5.0 sites. The Permission Wizard makes it easier to set up and manage Web sites that require authenticated access to content, lowering administrative overhead and total cost of ownership.

Finally, to keep in line with Internet standards, Windows 2000 Server provides full support for Digest Authentication. Digest Authentication offers the same features as Basic (unencrypted) password authentication, but involves a different way of transmitting the authentication credentials. Basic authentication sends passwords over the Internet as clear text; digest resolves this issue by obfuscating the password on the wire. This provides a considerable benefit to users with browsers supporting Digest Authentication, as it allows them to authenticate to an IIS 5.0 server without compromising their login credentials.

Internet Security Summary

Windows 2000 Server provides a complete standards-based Internet security infrastructure. It integrates with the Windows 2000 security environment to provide administrators with a single directory of users to manage. Additionally, once users are authenticated to a Windows 2000 domain, they don't need to log on to the Web server separately. It is the only solution to offer such key features as digest authentication. With its Permissions and Certificate Wizards, it is the easiest solution to administer.

Windows NT Server 4.0 provides full integration with the operating system security environment while also providing support for Internet standard security protocols such as basic and X.509 digital certificate authentication and SSL encryption.

Solaris 7 and Sun WebServer 2.1 supports standard authentication techniques but doesn't offer much beyond the basics. Furthermore, while access controls are available, these controls aren't integrated with the operating system.

Internet Services Administration

A robust Internet services management infrastructure is essential to deploying Internet-enabled technologies throughout an organization. A good Internet services implementation should offer centralized management and a user-friendly interface. Feature-sets should include the following:

- Locally executed administration tools.
- Browser-based administration tools for administrators working remotely.
- Command-line scriptable administration APIs to develop customized management solutions.
- Centralized administration for all Internet services.
- Ease-of-use tools to help automate difficult configuration tasks.

Solaris 7 Implementation Details

Internet services administration is provided through separate tools. For example, HTTP services are managed through the Sun WebServer Administration Console running on a server configured as an administration server. The Sun WebServer Administration Console is a browser-based administration tool that is implemented as a separate HTTP service running on the Web server. The administration service runs on a dedicated port and can be accessed by any member of the server administrator realm. This is a relatively non-comprehensive solution for several reasons. First, although browser-based remote administration is a useful feature, it is somewhat slow and unfriendly for administrators working locally, where a Windows-based solution might better suffice.

While Web-based administration capabilities are improving, many administrative tasks for the Internet services must be performed from the command line. Additionally, no integration between SMTP, FTP and HTTP service management is provided, requiring administrators to learn multiple tools to administrate Internet services on the Sun WebServer 2.1 platform.

Windows NT Server 4.0 Implementation Details

IIS 4.0 provides administrators with flexibility in management. IIS 4.0 can be managed through one of three different interfaces:

- **Windows-based** – Management and administration is provided via the MMC technology. MMC provides a user friendly graphical user interface and allows for management of both local and remote instances of IIS 4.0. Furthermore, administrators can manage the HTTP, FTP, SMTP, and NNTP services all from a single console.

- **Browser-based** –An HTML-based administration tool is also provided, allowing remote administration from any frame- and script-capable browser.

- **Command/Script Based** – IIS 4.0 introduces the Active Directory Services Interface (ADSI). ADSI provides a set of standardized, scriptable APIs to administer and configure all of the IIS 4.0 services. Using the combination of simple scripting and ADSI, administrators can automate common administrative tasks from the command line or via customized Web pages that can be accessed remotely. All IIS services – HTTP, SMTP, FTP, and NNTP – can be administered via ADSI. Several pre-authored command-line administration scripts are shipped with the product to provide command-line access to common administrative tasks. It should also be noted that the HTML administration pages shipped with the product are implemented entirely as ADSI administration scripts. ADSI brings several significant benefits to the customer including customizable administration and command-line administration – features that are unmatched in the Solaris 7 Internet services implementation.

IIS 4.0 also features full integration with the Windows NT Server 4.0 Performance Monitor application. With Performance Monitor counters for IIS, administrators have a considerable array of real-time monitoring tools to track virtually every aspect of an implementation’s performance and resource usage. Thresholds can be set for automated notification on certain performance and usage criteria, allowing a system administrator to be automatically notified of potential problem areas or periods of peak usage.

Finally, unlike previous versions of IIS, server configuration can be saved and restored at will. This brings administrators the benefit of total configuration management, including the ability to revert to previously saved configurations if undesirable settings are inadvertently applied.

Windows 2000 Server Implementation Details

Windows 2000 Server continues to support the flexibility of Web service management in Windows NT Server 4.0 with the addition of the following:

- **MMC Task Pads** enhance the already excellent MMC-based administration tool in IIS 4.0. Administrators are presented with a list of tasks that can be performed on each node or object under the IIS MMC snap-in. When an administrator selects a task, a wizard will walk the administrator through the selected task. This makes IIS easier to administer than prior versions, again lowering administrative overhead and total cost of ownership.

- **Additional Command-Line Administration Scripts** are shipped with IIS 5.0, providing even more manageability out-of-the-box from the server’s command prompt.

Internet Services Administration Summary

Windows 2000 Server includes everything that is shipped with Windows NT Server 4.0. In addition, Windows 2000 Server provides support for MMC Task Pads and easy-to-use wizards to automate the configuration of difficult tasks. Several more command-line administration scripts have been provided to give system administrators additional command-line capabilities without requiring them to custom-author their own scripts.

Windows NT Server 4.0 offers an easy-to-use, MMC-based tool for Windows-based administration. Browser-based administration is also provided for all services. A complete command-line administration suite is also provided which supports scripting for automation. Finally, with the Active Directory Services Interface (ADSI), administrators can easily create their own customized administration scripts and management applications, providing the ultimate in flexibility.

The management infrastructure provided in Solaris 7 to administer Sun WebServer 2.1 is limited to browser-based management, command-line administration and scripting. Windows-based administration is not available. There is no integration between administration tools for the SMTP, FTP and HTTP services. As such, Solaris 7 is the most difficult-to-manage solution.

Content Management and Logging Support

Content management and logging features are an important aspect of any Internet services implementation. Without them, the end-user's experience will not be as rich and administrators will not be able to adequately track usage patterns. Features to look for include the following:

- Redirection to provide a seamless end-user experience when content is relocated.
- Custom error pages to enhance the user's experience when problems are encountered.
- Custom footers to allow the appendage of common information (such as copyrights) to every page.
- Content indexing services to allow users to search site via keywords.
- PICS support to automatically rate server content via industry-standard RSAC ratings.
- HTTP Content expiration support to help improve client-side performance via content caching.
- WebDAV support to provide IETF standards-based Web publishing.

Solaris 7 Implementation Details

The Sun WebServer 2.1 shipped with Solaris 7 offers content management features including the following:

- **Redirection support,** allowing administrators to transparently redirect obsolete URLs to correct locations – either on local or remote servers. This feature eliminates the needless display of *not found* error messages or the need to maintain obsolete content and URLs when content is moved from one location to another, providing a considerably more seamless experience to the end-user.
- **Custom error support** allows the administrator to customize all of the standard HTTP error messages to provide additional information, corporate branding, or special instructions. This provides a richer and more seamless experience to the end-user and a friendlier user interface than unexplained HTTP error codes. It should be noted that only Unauthorized, Forbidden, Not Found, or Server Error can be customized. All other W3C-defined HTTP error conditions cannot be modified.
- **FrontPage server extensions** are supported via the Microsoft FrontPage services for Solaris.
- **Web-based file administration** is supported through WebNFS. WebNFS extends the standard features of NFS to the Web, enabling users to access data on the Web just as they access local data. WebNFS uses HTTP over TCP/IP to communicate and is designed to be more reliable and dynamic than FTP.

Additionally, WebServer 2.1 provides logging support for Web services. Logging can be configured on a per-site per-server basis. With regard to log file formats, most common log types are supported including the NCSA Common Log File Format, the W3C Extended Log File Format and the Extended Common Log File Format. Logging of email (SMTP, POP3 and IMAP4) services is handled by Solstice Internet Mail Server 1.0.

Windows NT Server 4.0 Implementation Details

Windows NT Server 4.0 provides a comprehensive content management solution as part of Internet Information Server 4.0. Features included with IIS 4.0 content management implementation include:

- **Microsoft Index Server 2.0,** an integrated content indexing solution for IIS 4.0 users. Index Server 2.0 provides a high-performance query engine to index Web content (such as HTML, text, Office, and other documents) on both local and remote directories. Index Server 2.0 allows for total customization of the user's search experience via Active Server Pages (ASP) technology. Numerous templates are shipped with Index Server 2.0 to allow users to get up and running quickly. In addition, Index Server is integrated with Windows NT Server security allowing users to see only the documents they have been granted the rights to view.

- **PICS Ratings,** integrated into IIS 4.0, allows users to automatically set and maintain RSAC content ratings for such things as nudity or violence at the server-side with an easy-to-use graphical interface. Nothing special needs to be inserted into the content itself in order for PICS ratings to function properly. With this feature, any PICS-compatible browser, such as Microsoft Internet Explorer, will automatically query the IIS server and disallow users access to content that has been restricted at the browser-level, negating the need for special content monitoring software.

- **Redirection support** in IIS 4.0 allows administrators to transparently redirect obsolete URLs to correct locations – either on local or remote servers. This feature eliminates the needless display of *not found* error messages and the need to maintain obsolete content and URLs when content is moved from one location to another, providing a considerably more seamless experience to the end-user.

- **Custom Errors** allow the administrator to customize all of the standard HTTP error messages to provide additional information, corporate branding, or special instructions. This provides a richer and more seamless experience to the end-user and a friendlier user interface than unexplained HTTP error codes. All W3C defined HTTP error conditions can be customized.

- **Custom Headers and Footers** can be set at the server side to allow administrator-defined HTTP headers and the inclusion of user-defined content on every page within a given site or directory. With this feature, administrators can set custom HTTP headers to allow pages to be cached by client browsers but not by proxy servers or search engines, giving the administrator the ultimate flexibility without requiring HTTP headers to be modified in individual pages. Custom footers allow a user-defined file to automatically be inserted within all pages within a given site or directory, allowing for commonly used information, such as copyright notices, corporate logos, or navigation bars, to be centrally administered without the need to modify or maintain individual Web pages.

- **Content Expiration** allows IIS 4.0 administrators to set an HTTP header determining how long a Web page should remain in a client's cache. This allows for centralized administration of caching information without the need to modify or maintain individual HTML pages.

- **FrontPage Server Extensions** are included with IIS 4.0. This allows the FrontPage Web site creation and management tool or any other FrontPage-capable client, such as the Microsoft Visual InterDev® Web development system, to create, manage, and maintain content on the server using easy-to-use, GUI-based tools. Additional capabilities added with FrontPage include hyperlink verification and security permissions management via FrontPage clients.

IIS 4.0 provides full logging support for all Internet services. Logging can be enabled or disabled on a per-site basis. Every directory and file can also be marked for inclusion or exclusion from access logging. Logging can be configured to automatically rollover to a new log file on a daily, weekly, or monthly basis, or when a log file reaches a set size in megabytes. Alternatively, all logging can be directed to a singular file on disk. Logging to any ODBC-compatible data source is also fully supported. With regard to log file formats, all popular log types are supported including the Microsoft IIS Log File Format, the NCSA Common Log File Format, and the new W3C Extended Log File Format. W3C logging also supports all extended attributes as defined by the W3C extended logging specification.

Windows 2000 Server Implementation Details

Windows 2000 Server platform extends the already strong content management infrastructure found in IIS 4.0. The major addition is WebDAV. The Web Distributed Authoring and Versioning (DAV) protocol is a ratified IETF extension to the HTTP 1.1 standard for exposing a hierarchical file storage medium, such as a file system, over an HTTP connection. With the WebDAV implementation of DAV on IIS 5.0, remote authors can easily access resources on the file system over HTTP. Administrators can allow remote authors to edit, move, search, or delete files and directories on the server all while using the HTTP protocol, IIS 5.0, and a DAV-compatible client such as Microsoft Internet Explorer 5.0 or Microsoft Office 2000.

Content Management and Logging Support Summary

Both Windows 2000 and Windows NT provide powerful content management solutions. While Windows 2000 Server stands out as the most complete solution because it is the only platform to support WebDAV, Solaris 7 does support WebNFS, which is a similar technology.

Windows NT Server 4.0 provides a comprehensive solution differentiated from Windows 2000 Server only by its lack of WebDAV support. Windows NT Server 4.0 features a comprehensive solution that includes content indexing, redirection, PICS ratings, custom errors, custom HTTP headers, custom page footers, and HTTP content expiration. Additionally, FrontPage Server Extensions are provided to allow distributed content authoring and management via the popular Microsoft FrontPage Web site creation and management tool. Logging support is also the most comprehensive – providing the largest variety of configuration options and support for all popular log file types including NCSA Common Log, W3C Extended Log, and the Microsoft IIS Log Format.

Solaris 7 and Sun WebServer 2.1 provide limited content management support. No support for PICS ratings, content indexing, or custom HTTP headers is included. Logging is not nearly as comprehensive, especially when looking at how logging is handled and controlled. Given the lack of features in comparison to both of the Microsoft offerings, or the Netscape Enterprise solution also marketed by Sun, it is less than a desirable solution.

Internet Server Scalability and Availability

It is important that server platforms be optimized for Web server performance. It's also critical that once a server has reached its full potential, organizations are able to expand from one server to a "farm" of Web servers. This guarantees that as the demand for Web server resources increases, organizations are provided with a solution to grow. In addition, as a Web site is distributed across one or more physical servers, the availability will increase as well. In order to facilitate this growth, scalability and availability services are required to provide automatic failover in the result of a server failure and automatic load balancing of HTTP requests between Web servers.

Solaris 7 Implementation Details

Solaris Easy Access Server lacks support for any integrated fault-tolerance and/or load balancing to benefit organizations that require more than a single Web server, or wish to provide higher availability by distributing their Web site across multiple servers. Additional products are available from Sun and third parties to provide these services to the Solaris platform.

On Solaris Enterprise Server, Sun Cluster and Solaris Resource Manager are available for handling clustering and load-balancing respectively. Sun Cluster supports 4-node clusters through an extensive GUI tool that helps ensure the reliability, availability and scalability. Solaris Resource Manager can improve application performance by dynamically allocating unused resource capacity and can also manage resources on a per user or per application basis.

Windows NT Server 4.0 Implementation Details

Available as a download for Windows NT Server 4.0 Enterprise Edition is the Network Load Balancing Service (NLBS). Based on technologies developed for the Convoy Cluster Software by Valence Research. NLBS installs as a standard network driver and service. It operates in a fully transparent manner to all server applications and TCP/IP clients. Clients can access a WLBS cluster as if it were a single computer. Under normal operations, NLBS automatically balances networking traffic between the clustered computers, scaling the performance of one server to the level required by the customer. When a computer fails or goes offline, NLBS automatically reconfigures the cluster to direct client connections to the remaining computers. When the offline system returns to service, it transparently rejoins the cluster and regains its share of the workload. This service compliments the Microsoft Cluster Server by providing both load balancing and fault-tolerance at the IP level, improving performance and availability for IP-based services.

Windows 2000 Server Implementation Details

Windows 2000 Server will continue to support the same Web farm clustering solutions for scalability and availability as outlined above for Windows NT Server 4.0. Performance enhancements in IIS 5.0 allow for significantly better performance on SMP systems or those hosting large numbers of sites. These enhancements allow many more sites to be deployed on a single server and provide for significantly better performance, reducing total cost of ownership.

Internet Server Scalability and Availability Summary

Where Internet services scalability and availability is a priority, Windows NT Server 4.0 and Windows 2000 Server provide Windows Load Balancing Services (NLBS). With NLBS, TCP/IP requests are automatically balanced between machines. In the event of a failure, user requests will be automatically redirected providing absolute availability.

The Solaris 7 scalability and availability solution is provided through Sun Cluster and Solaris Resource Manager, which must be licensed from Sun and installed separately from the operating system. Only the high-end Solaris Enterprise Server includes these products as a standard component.

Streaming Media Services

In today’s electronic commerce-dominated marketplace, audio- and video-enabled Web sites and applications for both internal and external use are becoming more important to corporate customers. Streaming media allows high quality audio and video to be delivered over the Internet even with low bandwidth, dialup connections. It is providing many organizations with new and exciting ways to communicate with customers, employees, and business partners. Popular applications of the technology include corporate communications, customer and sales support, news and entertainment services, and product promotions.

Solaris 7 Implementation Details

Solaris 7 currently offers no streaming media solutions of any kind. Solaris customers desiring to deploy streaming media solutions must look to other operating systems and solutions from third party vendors.

Windows NT Server 4.0 Implementation Details

Available as a free downloadable add-on, Windows Media Services is a comprehensive, scalable, streaming media solution for customers running Windows NT Server 4.0. Windows Media Services scales easily from low-bandwidth to high-bandwidth applications and features total integration with the Windows NT operating system and other Microsoft products.

Audio codecs range in bandwidth from under 5.0Kbps at the low end, 5.0Kbps to 8 Kbps in the middle range, and 96 Kbps at the high end for broadcast quality audio. Video codecs range from 28.8-56 Kbps at the low end for dialup users, 56-500 Kbps in the middle range for users with dedicated connections, and 300 Kbps to 8 Mbps at the high end for full-screen, broadcast quality video.

Windows Media Services is fully integrated with the security model present in Windows NT Server 4.0, allowing easy securing of content. Additionally, Windows Media Services integrates with Microsoft Site Server for usage analysis and Site Server Commerce Edition for pay-per-view, pay-per-minute, and other fee-based or advertising-based multimedia applications. Finally, Windows Media Services is also integrated with the Microsoft PowerPoint® presentation graphics program to deliver streaming slideshow presentations with integrated audio and video.

From a delivery perspective, Windows Media Services offers a variety of flexible options to deliver the broadcast to the client’s desktop. A fanout service is included that allows administrators to cost-effectively and easily distribute streams to other media servers, reducing network traffic over a Wide Area Network (WAN). In addition to traditional unicast (each client receives its own stream) deliver, Windows Media Services supports connectionless multicast, giving customers the ability to deliver a single stream to hundreds or thousands of clients simultaneously, greatly reducing the network bandwidth traditionally used in a unicast solution. In terms of capacity, Windows Media Services is currently the most cost-effective solution in the industry, supporting up to 1,200 simultaneous unicast clients on a single processor server with an Intel Pentium II 300 MHz processor.

In terms of media support, both live and staged events are fully supported. Windows Media Services supports the widely adopted Active Streaming Format (ASF) and Advanced Authoring Format (AAF) standards for streaming media.

Windows Media Services includes a full set of GUI based tools for administering the server-based services and for configuring and managing streaming media events. Command line and GUI-based tools are also provided for media clip encoding. The Windows Media On-Demand producer, co-produced by Microsoft and Sonic Foundry, provides an easy-to-use, GUI based tool for encoding, media management, and publishing using Windows Media Services.

Windows 2000 Server Implementation

Windows 2000 Server uses the same implementation of Windows Media Services currently available as a free download to users of Microsoft Windows NT Server 4.0. The server, administrative tools, and encoder components are integrated directly with Windows 2000 Server and are available as optional components in Windows 2000 Setup. Other media production tools remain freely downloadable over the Internet.

On the Windows 2000 Server platform, Windows Media Services directly benefits from the many enhancements to the networking and communications infrastructure. In particular, the Quality of Service (QoS) features help to ensure a more reliable, consistent delivery of streaming media than is available on Windows NT Server 4.0. Additionally, the performance enhancements to the TCP/IP protocol stack made in Windows 2000 Server will be of direct benefit to users of the Windows Media Services, providing for better throughput and increased reliability.

Streaming Media Services Summary

For customers who want streaming media solutions, Windows 2000 Server or Windows NT Server 4.0 are the only logical choices. Solaris 7 offers no streaming media solution of any kind, forcing customers to look to other operating systems and third party vendors. Of the two Microsoft platforms, Windows 2000 Server is the best choice, as the customer will benefit from operating system integration, enhanced performance, and enhanced reliability from the networking capabilities.

Management and Directory Services

Section Summary

Management features are among the most significant aspects of a network operating system. The true on-going cost of an operating system can easily be measured in terms of administrative overhead. Therefore, having an excellent management sub-system will greatly reduce total cost of ownership. Features to look for include a strong, hierarchical, scalable, and extensible directory; excellent management tools; infrastructure to manage application deployment and user desktops; and a comprehensive security implementation to ensure data safety.

Windows 2000 Server provides the most integrated and comprehensive management solution. Active Directory is the most scalable, standards-based, and extensible solution of the three directories evaluated. Particularly impressive is the Microsoft Management Console (MMC) technology, which is the basis of all management tools. The most complete infrastructure to manage applications and desktops is provided. It features many unrivaled capabilities such as user data management (IntelliMirror), application installation services (Windows Installer), or remote operating system installation – features that are unmatched by the other two solutions. Provided in both Windows NT Server 4.0 and Windows 2000 is a Common Information Model (CIM) based on the WBEM standard. Via CIM, WMI allows management applications used by the administrator to access and control all managed devices, drivers, services, and applications in a single, consistent way. The management scripting and directory-enabled development implementation is also the most comprehensive. Windows 2000 is the only solution to support Kerberos, TLS, and smart card authentication and provide an encrypting file system for security.

In the area of management and directory services, Solaris 7 provides a fairly comprehensive solution. Sun Directory Services 3.1 provides a fully LDAP-enabled directory service implementation, which supports legacy NIS systems and RADIUS for remote access. Sun provides the Solaris Management Console 1.0 (SMC) for GUI-based management of local and remote systems, which isn’t as powerful or intuitive as Windows NT or Windows 2000 management tools. One area in which Solaris 7 seems to outperform Windows NT and Windows 2000 is remote management. While it is true that many powerful command line tools are available to remotely manage systems, these command-line tools have no GUI counterparts for the most part. Further, with the addition of Windows Script Host and Netsh to an already strong line-up of command-line tools, Windows NT and Windows 2000 can match the command-line capabilities of Solaris feature for feature. Solaris 7 does provide a feature-complete implementation of security tools. Kerberos V5, TLS, Smart Cards, X.509 Certificate Servers, 40-bit and 128-bit SSL are all available. However, there is no single tool or location that allows the administration of all aspects of security management.

Although it offers a good management infrastructure, Windows NT Server 4.0 falls into last place by its dated, non-extensible directory. It lacks key features in the other solutions, such as application distribution and management, user data management, and advanced authentication or encryption options. Its strongest points are GUI tools, MMC support, WBEM support, management scripting, and an excellent desktop management toolkit.

Feature Table

Feature	Solaris 7	Windows NT Server 4.0	Windows 2000 Server
Directory Services			■
Hierarchical Directory	■	□	■
Supports Partitioning	■	□	■

Multi-Master Replication	□	□	■
Catalog Services	□	□	■
Real-time Catalog/Directory Access	□	□	■
Same Security Model for Catalog & Native Directory	□	□	■
LDAP Support	■	□	■
Native LDAP Integration	■	□	■
LDAP & Directory Utilize Similar Naming	■	□	■
All Directory Interfaces LDAP-exposed	■	□	■
LDAP Uses Same Directory Security Model	■	□	■
DNS Support	■	■	■
Single Network Sign-On	■	■	■
Inheritance Model	Static	Static	Enhanced, Real-time Static
Included Development Model	□	□	■
Synchronization & Consolidation Platform	□	□	■
Management Infrastructure			
Command-line Administration	■	■	■
Windows Administration / GUI Administration	■	■	■
Java-based Administration	■	□	□
Integrated Management Tools	■	■	■
Extensible Management Tools	■	■	■
SNMP Support	■	■	■
Management Scripting	■	■	■
Java Scripting Support	■	■	■
Visual Basic Scripting Support	□	■	■
JavaScript Scripting Support	■	■	■
Extensible Scripting Engine	□	■	■
WBEM Support	■	■	■
Application Deployment Services	■	□	■
Application Installation Services	■	□	■
Group Policy Services	□	■	■
Desktop Change & Configuration Management			
User Data Management Services	□	□	■
Synchronization Between Client/Server of User Data	□	□	■
Desktop Application Management	■	□	■
Advertised Applications	□	□	■
Assigned Applications	□	□	■
Published Applications	□	□	■
User Settings Management	□	■	■

Define Desktop Settings for Users	□	■	■
Roaming User Support	□	■	■
Lock-down of User Desktop Settings	□	■	■
Remote Operating System Installation	■	□	■
Security			
Kerberos Authentication	■	□	■
Transport Layer Security (TLS) Authentication	■	□	■
Smart Card Support	■	□	■
X.509 Certificate Server	■	■	■
Certificate Server / Directory Integration	■	□	■
Centralized Security Management	■	■	■
40-bit SSL Support	■	■	■
128-bit Strong SSL Support	■	■	■
File System Encryption	■	□	■

Directory Services

Directory services within networked computing environments are not a new concept. Many organizations have implemented white pages to make basic information available to all employees. E-mail applications have used directories as address books. Within the network operating systems, directory services show that it is possible to simplify network management tasks by storing all information in a centralized directory. With today’s network operating systems, directory services must be capable in the following roles:

- **User and Network Resource Management** by providing a scalable, hierarchical information repository to simplify tasks such as delegating administrative privileges and locating network resources such as printers.
- **Security Authentication and Authorization Services** by providing flexible authentication and consistent authorization services that protect data and minimize barriers to doing business over the Internet.
- **Directory Consolidation** by reducing the number of directories companies need to improve sharing and enable common management of users, computers, applications, and devices.
- **Directory-enabled Infrastructure** by enabling elements such as networking hardware and shared file systems to offer enhanced service quality and greater functionality through access to information about users (and their roles), machines, network elements, and policies stored in the directory.
- **Directory-enabled Applications** by enabling simplified application configuration and management and greater functionality and synergy with other directory-enabled components of the network-computing environment.

However, without a solid technical foundation, no network operating system will be capable of performing the aforementioned roles. As such, the following technical criteria must be considered when evaluating a network operating system based on directory services:

- **Scalability** – The various roles that directory services play require the storage and replication of millions of objects efficiently and cannot require complex configuration of servers. A directory partition (or division) must scale to hold at least 1,000,000 objects. And objects should be easily queried and located within the directory. Catalog services should be provided to expedite object search and retrieval; latency should be low.

- **Internet Standards** – Given the wide range of ways that directory services will be used, often from across corporate and geographic boundaries, directories must locate and access objects completely via Internet standards such as the Domain Name Service (DNS) and the Lightweight Directory Access Protocol (LDAP). All directory services, not just a subset, should be totally exposed via LDAP and DNS to achieve true standards compliance.
- **Flexible and Simple Security** – Along with the desire to increase access to directories is the need to protect corporate resources without placing design restrictions on networks or increasing management complexity. Access rights via catalog services and LDAP should not be computed differently than when the directory is accessed natively. Full group support should be provided and no performance implications should be imposed on creating groups that span multiple directory partitions.
- **Consolidation** – Because most organizations will not be able to eliminate all of the application-specific directories that they use today, multi-purpose directories must enable consolidation and provide synchronization facilities to minimize duplicated administrative efforts. Additionally, scalability should ensure that bringing large numbers of objects into the directory raises no significant performance issues.
- **Application Development Environment** – To attract software developers, directories must be full-featured, easy to use, with exposed APIs, and platforms that provide a comprehensive and simple-to-use development environment.

Solaris 7 Implementation Details

The primary name resolution service supported by Solaris 7 is Sun Directory Services 3.1. Sun Directory Services is a complete multi-protocol directory for storing user, resource and configuration information. Directory data information is object-based and stored in a directory tree structure. Classes of objects can be accessed in the directory through the hierarchy provided by the directory tree. For example, you could use the directory to look up the email address of a user at the Seattle office even though you are in the London office. This information could be accessed through LDAP or via the Web/LDAP gateway service. Sun Directory Service also supports RADIUS for remote authentication and NIS for applications that use NIS naming services.

Directory Schema and Controls

Information in the directory is organized according to a predefined directory schema. This schema can be modified, which allows you to customize the directory environment. Access to information in the directory is controlled through access control lists which provide five basic modes:

- **None** – No access
- **Compare** – Allows comparisons of values but doesn’t grant read access.
- **Search** – Allows searching of the directory by reading distinguished names (DNs).
- **Read** – Provides read access to the directory.
- **Write** – Provides write access to the directory.

These controls are similar though less elaborate to the controls available in Windows 2000. Directory data can be managed through any Web-enabled browser or by running the management applications, which include Administration Console for local and remote administration and Deja for updating the directory.

Directory Architecture

Sun Directory Services supports LDAP v3 as defined in RFC 2251 and LDAP servers are a core part of the directory architecture. Directory information is replicated throughout the network using an LDAP replication service. Data can be replicated at the subtree, object or property level. Two replication daemons are provided. The dspushd daemon pushes updates from a master server to a slave server and in this way, the master server manages the replication schedule. The dspulld daemon allows a slave server to pull updates from a master and in this way secondary servers manage the replication schedule.

The master-slave replication model is also referred to as the single master replication model. There are many problems inherent in this model. The biggest problems is that outdated data may be retrieved by client applications. Another major problem is that a single server is responsible for processing and replicating changes, which provides a single point of failure and places a heavy burden on the master server. In contrast, the multimaster model used in Windows 2000 gives all servers equal responsibility—any server can process and replicate changes.

Sun Directory Services also supports NIS replication. This type of replication ensures NIS information is maintained and updated throughout the network. NIS services and replication are handled by NIS servers, which are another component of this architecture. With a maximum table size of 50-60,000 entries, NIS servers are not designed to handle large networks or large information loads. NIS support is primarily made available for legacy systems.

NIS services are handled by the dsservd daemon, which can act as an NIS master or an NIS slave. In the role of a master server, dsservd propagates NIS tables to a slave NIS server. In the role of a slave server, dsservd receives propagation requests. Replication between an integrated LDAP/NIS server and a legacy NIS server is handled through a proxy daemon, dsypxfrd.

The final server component in this model is a RADIUS server. Remote Access Dialup User Service (RADIUS) is used to authenticate remote users. The RADIUS server functions are handled by the dsradiusd daemon.

Directory Management

Sun Directory Services also includes the following Java tools that you can run as applets in any Java-enabled Web browser, or as applications:

- Administration Console for local or remote configuration and administration.
- Java Directory Editor (Deja) for updating the directory database.

Two SNMP agents are available for obtaining management statistics. The dsnmpserv agent supports the Mail And Directory MANagement (MADMAN) standard specified in RFC 1565 and RFC 1567. The dsnmprad agent supports the RADIUS Accounting Server Management Information Base (MIB).

Directory service security is handled through LDAP, RADIUS and password encryption techniques. The LDAP server component supports Simple Authentication Security Layer (SASL) and Secure Socket Layer (SSL). However, SSL security is available only if SSL and Sun Certificate Manager are installed on the directory server. The RADIUS server component uses MD5XORing shared secret keys to authenticate remote users. Directory entries can also be protected and password encrypted. In this case, the standard crypt (3) encryption algorithm is used.

Windows NT Server 4.0 Implementation Details

Because Widows NT Directory Services (NTDS) is not a hierarchical directory, the concept of partitioning a portion of the directory, as such, does not exist on this platform. Instead, flat user account databases (domains) are used – which scale well up to 25,000 users (including a user account and machine account for each user – 50,000 objects total). Typically, customers of Windows NT Server 4.0 running NTDS use multiple domains with trust relationships to divide their network and provide roughly similar functionality to partitioning at a high level.

Windows NT Directory Services (NTDS) does not provide an implementation of directory catalog services. Nor does Windows NT Server 4.0 support the Lightweight Directory Access Protocol (LDAP) as part of the base operating system. Support for the Domain Name Service (DNS) is provided, but no real integration with Windows NT Directory Services (NTDS) exists, leaving customers of Windows NT Server 4.0 with no Internet-standards based directory access. Other features of the Windows NT directory service implementation follow.

Security Services

- **Authentication –** Windows NT Server 4.0 provides integrated LAN Manager authentication, providing challenge/response authentication and single network sign-on. Once a user has authenticated to Windows NT Directory Services (NTDS), authorization is performed in a consistent fashion across files, applications, and other resources.
- **Inheritance** – Windows NT Server 4.0 implements traditional static inheritance of access control behaviors. Under this model, access control behaviors are computed and attached directly to the child object when some access right to a parent object is changed. An administrator does not necessarily have to make explicit changes to each child object when an access right of a parent object is changed.
- **Groups** –Windows NT Server 4.0 fully supports the creation of groups within NTDS. As with the Active Directory implementation found in Windows 2000 Server, there are no significant performance implications from the creation of groups whose memberships span multiple domains.

Synchronization and Consolidation

Windows NT Directory Services (NTDS) provides no synchronization features as part of its implementation. As such, users cannot perform such tasks as request change lists, making it a poor choice on which to build replication-sensitive directory-enabled applications.

Windows NT Directory Services (NTDS) on the Windows NT Server 4.0 platform is a non-extensible directory. Customized objects cannot be created within Windows NT Domains. Only user and group data can be stored in NTDS. As such, Windows NT Server 4.0 is not a solution capable of providing a consolidation platform for corporate information.

Development Environment

Windows NT Server 4.0 exposes an API set allowing developers to build solutions that leverage the Windows NT Directory Services (NTDS) for authentication and security. Because Windows NT Server 4.0 can support a large number of users per domain (partition), it is a good solution for building applications that use NTDS solely for the purpose of authentication. However, as the directory is not extensible and cannot store customized information, it is not a platform on which sophisticated directory-enabled applications can be constructed.

Windows 2000 Server Implementation Details

Through its multimaster domain structure, Windows 2000 provides the most robust directory service. With multimaster, any domain controller can process and replicate directory information. Unlike Sun Directory Services, replication of the directory is automatic. You don’t need to configure replication manually, but can optimize replication using bridgehead servers. Bridgehead servers are designated to handle replication between sites, which places the bulk of the intersite replication burden on a specific server rather than on any available server in a site.

Directory Organization

The Active Directory service organizes directory information using a directory tree, which is an object-based hierarchy of information. To ensure data is organized and accessible, Active Directory provides both physical and logical structures for network components. Sites are used to map the physical structures of the network. Site mappings are independent from logical domain structures and because of this there is no necessary relationship between a network's physical structure and its logical domain structure. Logical structures are organized into domains, domain forests, and domain trees. A domain is a group of computers that share a common directory; domain trees are groups of domains that share a contiguous namespace; domain forests are groups of domain trees that share common directory information.

The boundary of a partition within Active Directory is a Windows 2000 Domain. All of the entities within the domain that have associated Active Directory objects will be accessible within a single partition. Because Active Directory supports multimaster replication, a full read/write replica of the partition will be available on all domain servers in the domain, even when the domain spans multiple physical sites.

Active Directory partitions use an efficient indexed data store, which holds information about all entities in a domain. As such, domains can easily contain millions of users and machines. Replication is highly optimized, featuring advanced techniques such as data compression and automatic use of bridgehead servers to reduce the need to create domain boundaries on a physical location basis due to the restricted availability of network bandwidth. Bridgehead servers ensure that replication traffic between sites and across lower network links is performed efficiently. Updates travel once between bridgehead servers, which then propagate the updates to other domain controllers in the site.

Directory Structure

Active Directory on Windows 2000 Server provides a mechanism called a Global Catalog to enable administrators to build a specialized directory containing a subset of object attributes that are of interest beyond a single domain. The Global Catalog builds off of the concept of trees and forests of related domains in Windows 2000 Server to determine how domains participate in the Global Catalog process.

In particular, Active Directory enables administrators to specify which domain controllers in a given domain should hold global catalog information in their Active Directory partitions. Then, administrators specify which object attributes should be replicated to the Global Catalog using the Active Directory Schema Manager. When any object in the tree or forest is added or updated, information about the update is propagated automatically, using the same replication technologies as within a domain, to all domain controllers that are configured to hold Global Catalog information.

Global Catalogs are updated simultaneously with other replication cycles to ensure that catalogs stay consistent with their underlying domain-based objects. Additionally, they are kept within Active Directory partitions themselves to enable a single, unified way of accessing all Active Directory objects. Finally, objects and attributes in the Global Catalog retain their original access control lists to ensure that catalog operations do not compromise security.

Internet Standards Support

Microsoft designed Active Directory from the outset as a native Lightweight Directory Access Protocol (LDAP) Version 3 server. As such, LDAP-based requests are processed directly without translation against the Active Directory data store. Active Directory also exposes all of its functionality via LDAP interfaces. For example, Active Directory provides LDAP-based support for schema management, change history, and query scoping. More importantly, because of Active Directory’s inherent scalability, it is well suited in environments where large numbers of objects are hosted via a single partition – commonly used in such scenarios as corporate address books or product catalogs. Active Directory is easily capable of hosting over one million objects in a single, fully indexed partition.

Likewise, Microsoft designed the Active Directory name space around the Internet standard for name resolution – the Domain Name Service (DNS). Active Directory domain names are the same as DNS domain names. Because domains have a one-to-one relationship with Active Directory partitions, Active Directory name spaces can be located natively via DNS. Furthermore, an Active Directory object's fully distinguished name contains the DNS name of its partition, is globally unique, and completely describes how to find the object in a company's intranet or across the entire Internet.

Security Services

- **Authentication** – Active Directory supports multiple security authentication protocols including LAN Manager (NTLM), Kerberos, and X.509 certificates. Support for Internet-based standards such as X.509 and Kerberos allow Windows 2000 Server to function well in Internet-connected environments and scenarios. Active Directory uses a modular approach to authentication, making it easy to add additional authentication protocol support. Once a user has authenticated to Active Directory, authorization is performed in a consistent fashion across files, applications, and other resources.

- **Inheritance** – The Active Directory service in Windows 2000 Server implements a sophisticated form of static inheritance. Each child object has an access control list attached that contains the summary of all access rights that are either specifically assigned to the object or inherited from its parent. Active Directory recomputes child access rights automatically when a parent object's rights are changed. Then, only the change to the parent object is replicated between domain controllers and global catalogs. The child access rights are then recomputed on each domain controller – a fast and local operation.

- Active Directory inheritance has been implemented in this fashion because directories must be optimized for read (versus write) behavior. Active Directory pays the price of recomputing access control behaviors once (at the time a parent object is changed) rather than on every read operation. The net effect to the user of true dynamic inheritance and the way Active Directory implements inheritance is the same. However, the net effect to organizations deploying Active Directory is faster access to information stored in the directory for their network users.

- **Groups** – Active Directory implements security groups in such a way that it is possible (and efficient) to create groups that span organizational units within a partition and across domains that are part of a forest or a tree. This makes it easy for administrators to create groups that include members regardless of their location in a partition or the domain to which they belong.

Synchronization and Consolidation

Active Directory provides synchronization features that enable companies to use it immediately as their focal point for centralized management and single sign-on infrastructures, while transitioning away from existing directories. In particular, Active Directory includes an LDAP-based interface for requesting lists of all object additions and updates since a given point in time. These interfaces make it easy for applications to synchronize objects in different directories without resorting to inefficient techniques such as tree walking or monitoring replication traffic. Additionally, after the release of Windows 2000 Server, Microsoft expects to offer an additional product that will use Active Directory change notification mechanisms to synchronize Active Directory objects with corresponding objects in other directory services.

As previously mentioned, Active Directory provides scalability up to millions of objects in a single partition. This enables it to be easily utilized as a consolidation point for other application-specific directory services and object stores including:

- Microsoft Exchange Server.
- Microsoft Message Queuing Services.
- Microsoft Commercial Internet Services.
- Other third-party meta-directory vendors.

Development Environments

Developers have two different sets of interfaces for building directory-enabled applications based on Active Directory. These include:

- **Lightweight Directory Access Protocol (LDAP)** – Active Directory has been designed as a 'native' LDAP server. LDAP-based requests are processed directly without translation against the Active Directory data store. Active Directory also exposes all of its functionality via LDAP interfaces.
- **Active Directory Services Interfaces (ADSI)** – To make it easier to write directory-enabled applications that access Active Directory and other LDAP-enabled directories, Microsoft developed ADSI. ADSI is a set of extensible, easy-to-use programming interfaces based on Microsoft Component Object Model (COM) that can be used to write applications to access and manage Active Directory and other LDAP-based directories. ADSI abstracts the capabilities of directory services from different network providers to present a single set of directory service interfaces for managing network resources. This greatly simplifies the development of distributed applications, as well as the administration of distributed systems. Developers and administrators use this single set of directory service interfaces to enumerate and manage the resources in a directory service, no matter which network environment contains the resource. Thus, ADSI makes it easier to perform common administrative tasks, such as adding new users, managing printers, and locating resources through the distributed computing environment. Combining the wealth of tools that support COM, ADSI makes it easy for developers to directory-enable their applications using any language that supports COM.

Beyond ADSI, Active Directory provides developers with the comprehensive feature-set they need to build powerful directory-enabled applications that deliver great functionality and enable lower TCO. Some of the features included with Active Directory include the following:

- **Group Policy Integration** – Group policy features enable administrators to define sets of applications, including specific configurations, that users should have available based on their role in the company, the domain of which they are a member, and the security groups to which they belong. When a user is moved into an organization or added to a Windows NT security group, applications can be installed and configured automatically – helping to lower installation and configuration costs dramatically.
- **Service Publication** – Active Directory enables applications to publish the names and locations of service they provide so that clients can locate and use services dynamically. This allows administrators to reconfigure servers for optimal response times and higher availability without having to update clients.
- **Directory Object Extension** – Active Directory provides the ability for applications to add new types of objects and to extend existing objects with new attributes. Thus, Active Directory can be a consolidation point for reducing the number of directories that companies have. Benefits include improved information sharing and common management of users, computers, applications, and directory-enabled devices.
- **ADSI Extension Model** – ADSI provides a feature called the ADSI Extension Model that allows application developers to associate COM-based business rules with objects stored in Active Directory. This provides a consistent and simple way for developers and administrators to interact with an application and its objects. The Extension Model also makes it easy to invoke methods across groups of objects to simplify administration.

- **Active Directory Class Store** – The Active Directory provides a section of the directory tree called the Class Store to store the names and locations of COM objects installed on the network. COM uses the Class Store to locate and install the COM objects that users are allowed to use on their machines automatically. This can lower the total cost of ownership of COM-based applications by simplifying client configuration and administration.

Directory Services Summary

Active Directory is a feature-complete and scalable directory services implementation. Scalability is excellent – up to one million objects per domain (partition). Partitions use indexed data store for fast object retrieval, ensuring excellent performance. Replication between sites and over slow network links is optimized, ensuring that Wide Area Network (WAN) bandwidth will be available in Active Directory environments. Catalog services are provided in the form of the Global Catalog. The Global Catalog is updated simultaneously with other replication cycles, ensuring low latency. A single data store and set of access methods is used for both the partitions and catalogs, ensuring that information from the directory is always consistent and up-to-date.

Full support for the Lightweight Directory Access Protocol (LDAP) is provided because Active Directory was designed from the outset as a native LDAP implementation. No request translation services are necessary and access control rights are consistently implemented via both LDAP and native directory access. LDAP-based access is present for all services. Domain Name Service (DNS) support is equally integrated, as Active Directory uses DNS natively as its name space solution for object location and access. The Global Catalog enforces complete object- and attribute-level security, meaning that it is an excellent choice when used as a reference for authentication. Full group support is provided and there are no performance implications of defining security groups that span domains (partitions).

Because of its inherent scalability and superior catalog performance for queries, Active Directory is an excellent solution on which to consolidate large directories without administrative complexity. Integrated LDAP-based change history facilitates the Active Directory use as a meta-directory platform. As such, today it is being utilized as the basis for the information/object stores in several new Microsoft products including the next releases of Exchange, Message Queuing Services, and the Microsoft Commercial Internet Services (MCIS) package. Active Directory is also easily extensible, providing the COM-based Active Directory Services Interface (ADS) for simplified development. LDAP also exposes access to all Active Directory features, making it an excellent choice on which to develop Internet standards-based solutions. Finally, its inherent scalability allows the development and deployment of large-scale directory-enabled applications that can store, access, and manage millions of objects without application-level complexity.

Sun Directory Services 3.1 adds a fully LDAP-enabled directory service implementation to the Solaris 7 package. The service provides support for standards such as LDAP and RADIUS, but lacks true integration with the operating system. Some directory maintenance is possible via the Java based directory editor. Otherwise management is done via the command line. A Web interface to the directory is also provided, but not recommended for maintenance or configuration uses.

Of the three solutions evaluated, Windows NT Directory Services (NTDS) on the Windows NT Server 4.0 platform is the most dated directory services solution. Because it is not even a hierarchical and extensible directory, it is not fair to compare it directly against Active Directory in Windows 2000 Server and Sun Directory Services in Solaris 7. Its strongest point is its centralized store for user and group management; allowing customers to provide single sign on services across enterprise networks and applications. In all other areas, it simply cannot be directly compared, as it does not offer functionality similar to that present in NDS and Active Directory because of the fundamental architectural differences.

Management Infrastructure

The management infrastructure provides the tools and capabilities to manage all aspects of the network operating system. With the focus on reducing total cost of ownership in many information technology environments, a comprehensive, easy-to-use solution is essential when making a network operating system choice. Features that should be included in any management infrastructure include the following:

- **Management Presentation Services**, which includes easy-to-use, consistent graphical administration tools for all operating system services, user interface customization features, and an extensible API set for the addition of enhancements and new capabilities.
- **Management Instrumentation Services** to monitor the ongoing operations of the network operating system. All implementation should include full SNMP support and an implementation of the Desktop Management Task Force's Web-Based Enterprise Management specifications.
- **Management Scripting Services** should include a comprehensive, multilingual scripting model on which scripts can be easily authored to provide automated administration scripts that can be executed in batch or customized management interfaces.
- **Group Policy Services** to manage the experience for clients of the network operating system. All implementations should provide a policy editor in which an administrator can set and deploy user access policies across the network; a security configuration editor in which security policies can be set and globally enforced to restrict access to various aspects of the network operating system and its clients; and application deployment services to centrally install applications across the network and provide self-configuration and healing capabilities once packages are installed on client workstations.

Solaris 7 Implementation Details

Management services aren't a strength of the Solaris operating system. The power of Solaris is often tied to the command-line, which is where most management utilities are executed. Solaris has an extensive set of command-line utilities for managing local and remote systems—and remote systems management is particularly strong from the command line. Unfortunately, command-line utilities are arcane. They're often more complex than the graphical counterparts and often require considerable expertise for proper usage.

Management Presentation Services

Management presentation is handled via the Solaris Management Console 1.0. The SMC is used to view applications and servers, and to start administration tools. There are two views possible: Application View and Server View. The Application View shows the applications that are installed in the SMC and can be launched from this point. Server View shows all servers that are running the SMC application, their status and available applications. You can launch any of the visible applications on a selected server. There are few points of comparison between the Solaris Management Console and the Microsoft Management Console. There is no commonality of interface between the applications launched from the SMC (in fact, they are just the applications that would be launched from the command line or the AdminSuite), nor can the user create custom views of the available tools, short of reconfiguring the entire SMC.

Still, all Solaris administration tools can be integrated into and run from the SMC. The SMC supports single login and enterprise-wide authentication. This allows administrators to manage applications, servers and services without having to provide passwords each time. SMC also supports HTTPS and SSL for secure communications with remote systems.

Solaris Administration wizards can also be run from the SMC. The six wizards provided with Solaris 7 are:

- Change Root Password.

- Default Router Modification.
- DNS Client Configuration.
- DNS Server Configuration.
- Network Connection Configuration.
- Shutdown/Restart Computer.

Management Instrumentation Services

Solaris 7 provides solid support for the Simple Network Management Protocol (SNMP) for certain key services. In particular, the dsnmpserv and dsnmprad agents make it possible to obtain management statistics for Sun Directory Services. Solaris 7 also provides full support for the Web Based Enterprise Management (WBEM) specification set forth by the Desktop Management Task Force (DMTF). WBEM uses technologies like the Common Information Model (CIM) and Extensible Markup Language (XML) to manage servers and the operating system.

Sun's implementation of WBEM, called Solaris WBEM Services, is Java-based and supports CIM schema and the Desktop Management Interface. Sun also provides an SDK for WBEM, called Sun WBEM SDK. Together these products provide a fairly complete set of tools for developing management applications. Client APIs and provider APIs for creating management applications are all apart of the WBEM SDK.

Management applications use the Solaris WBEM providers to communicate information between the operating system and an object manager (CIM Object Manager). Essentially, the object manager provides event handling for managed objects. These managed objects are described through Solaris Schema and placed in the CIM repository using the Managed Object Format Compiler.

Solaris WBEM Services support HTTP and LDAP as their communications protocols. Sun WBEM also supports SNMP, making it a solid management instrumentation offering.

Group Policy Services

A function similar to group policies can be created in Solaris 7 by using the creation of specific user realms with security and access policy tied to user membership within those realms.

Windows NT Server 4.0 Implementation Details

Management services in Windows NT Server 4.0 are very strong, yet Windows NT is often perceived as not having strong remote management capabilities. This perception is often the result of users having familiarity with early versions of Windows NT Server and not with the latest version. In Service Pack 4 and later, Windows NT Server supports the Microsoft Management Console for GUI-based administration, an extended command shell and the Windows Script Host—each of which can be an extremely powerful tool for managing local and remote systems.

Management Presentation Services

Windows NT Server 4.0 provides an extremely rich set of graphical management tools for its management presentation services implementation. The most key system management tools included with Windows NT Server 4.0 include the following:

- **Disk Administrator**, which is used to manage storage devices on the Windows NT Server 4.0 platform. With it, drive letters can be assigned, partitions created and deleted, and stripe sets and volumes managed.
- **Control Panel**, which provides management of system services, network configuration settings, printers,

and hardware configuration settings.

- **Event Viewer**, which is used to monitor the system's event logs to facilitate an administrator tracking activity on the system.
- **User Manager**, which can be used to manage user and group accounts as well as system policies.
- **Performance Monitor**, which is used to monitor performance graphically in real-time and signal an alert when user-defined performance thresholds are met or exceeded.

Additionally, the next-generation Microsoft Management Console (MMC) technology has been ported to the Windows NT Server 4.0 platform. MMC is available with the Windows NT Option Pack, Microsoft SQL Server 7.0, and selected components in the Windows NT Server 4.0 Service Pack 4. It provides a next-generation, standardized graphical user interface to manage system services. On the Windows NT Server 4.0 platform, many core services can now be managed via MMC including the following:

- Internet Information Server 4.0
- Transaction Server 2.0
- Index Server 2.0
- SQL Server 7.0

For more details regarding the technical implementation of MMC, please see the Management Presentation Services module under the Windows 2000 Server Implementation Details in this section of this document.

Management Instrumentation Services

Out of the box, Windows NT Server 4.0 provides integrated support for SNMP. This allows any SNMP standardized management package to connect with and track the ongoing performance of systems running Windows NT Server 4.0.

Additionally, with the debut of Service Pack 4 for Windows NT Server 4.0, the full support is provided for the WBEM specification. For details on WMI, please reference the Management Instrumentation Services module under the Windows 2000 Server Implementation Details in this section of this document.

Management Scripting Services

A full management scripting implementation is provided on the Windows NT Server 4.0 platform with the debut of the Windows Script Host in the Windows NT Option Pack. The WSH feature's implementation on the Windows NT Server 4.0 platform is essentially identical to that shipped with the included WSH functionality found in Windows 2000 Server. For specific technical details regarding the WSH implementation, please reference the Management Scripting Services module under the Windows 2000 Server Implementation Details in this section of this document.

Windows NT Server 4.0 with Service Pack 4 or later also supports an extended command shell. The command shell provides the tools you need to manage local and remote systems, such as AT for creating schedule jobs, NTBACKUP for creating backups, and the NET commands for managing user accounts, groups, services and systems. The new shell programming language supports variables, control flow, conditional statements, procedures and more, making it easy to script most administrative tasks. To script more complex tasks or to gain the benefits of a full-blown scripting language, Windows Script Host provides a full-featured alternative.

Group Policy Services

Windows NT Server 4.0, especially with the enhancements in Service Pack 4, provides rudimentary Group Policy management capabilities as part of the operating system. The solution is composed of the following elements:

- **System Policy Editor,** included with the core Windows NT Server 4.0 product. It allows administrators to centrally define user and computer settings for Windows NT-based clients. Using System Policy Editor, administrators can create system policies to control user work environment and actions, and to enforce system configuration settings for all computers running Windows NT on the network.

- **Security Configuration Editor**, as found in Windows 2000 Server, has been ported to the Windows NT Server 4.0 platform and released as part of the freely available Service Pack 4 update. It allows system administrators to consolidate all security related system settings into a single configuration file. These security settings may then be applied to any number of Windows NT-based machines. For more information regarding the technical details of the Security Configuration Editor implementation, please see the paragraph describing the Security Configuration Editor in the Group Policy Services module under the Windows 2000 Server Implementation Details in this section of this document.

Windows 2000 Server Implementation Details

Windows 2000 supports and extends the management services found in Windows NT. The operating system has a tightly integrated management service framework and strong support for remote management.

Management Presentation Services

The MMC is an ISV-extensible, common console framework for management applications on the Windows platform. MMC was expressly developed to provide a consistent, easy-to-use presentation of management information to system administrators in an effort to lower administrative overhead and total cost of ownership (TCO).

The console itself is a Windows-based multiple document interface (MDI) application that heavily utilizes Internet technologies. The MMC does not provide any management behavior, but it provides a common environment for snap-ins, which are written both by Microsoft and independent software vendors. The snap-ins themselves provide the actual management functionality.

The MMC interfaces permit the snap-ins to integrate with the console. These interfaces only deal with user interface extensions. The author of the snap-in determines the functionality of each snap-in. The relationship with the console is that it shares a common hosting environment and cross-application integration. Development framework to build MMC-based applications is provided as part of the Windows Software Developer Kit (SDK) and is available for general use.

Administrators can create custom management consoles by combining various snap-ins and then saving the console for later use or sharing with other administrators. This model provides the administrator with efficient tool customization and the ability to create multiple tools of different levels of complexity for task delegation, among other benefits. Administrators can define the configuration of snap-ins to manage a particular problem, save the configuration as a compound file, and then send it to others as the de facto environment in which to manage the scenario at hand.

Although it was introduced in Windows NT Server 4.0, the implementation in Windows 2000 Server contains numerous snap-ins to accomplish common management tasks. Some examples of MMC snap-ins are:

- **Computer Management** snap-in is an administrator’s computer configuration tool. It is designed to work with a single computer, and all of its features can be used from a remote computer, allowing an administrator to troubleshoot and configure a computer from any location on the same network. It provides access to the base Windows 2000 Server tools (viewing events, creating shares, managing devices, and so forth), but also dynamically discovers what server services and applications there are to administer.

- **Disk Management** snap-in is a graphical tool for managing disks that replaces the Disk Administrator from prior versions of Windows NT. It supports partitions, logical drives, and the new dynamic volumes. It contains shortcut menus and wizards to simplify creating volumes as well as initializing and upgrading disks. All changes are dynamic and can be implemented without rebooting the system or interrupting users.
- **System Service Management** snap-in allows administrators to stop, start, pause, and resume services on local and remote computers, replacing the Service Control Panel application from previous versions of Windows NT. Service monitoring support is also provided to allow Windows 2000 Server to automatically restart the service, run a script or .exe, or reboot the server in the event that a mission-critical service fails.
- **Device Manager and Hardware Wizard** provides a snap-in that allows administrators to configure devices and resources on the system. Adding new hardware, changing device properties, unplugging or ejecting devices, and resolving hardware conflicts can all be easily accomplished within this module.

Management Instrumentation Services

Windows 2000 Server supports the Desktop Management Task Force (DMTF) Web-Based Enterprise Management (WBEM) through built-in technology known as the Windows Management Instrumentation. This provides a unifying mechanism for accessing and associating information from many management sources.

WMI in Windows 2000 Server has both a Kernel-Mode and User-Mode component. WMI unifies management instrumentation from many diverse sources into a single model and expresses the information using a WBEM-compliant data schema known as the Common Information Model (CIM). Via CIM, WMI allows management applications used by the administrator to access and control all managed devices, drivers, services, and applications in a single, consistent way. At the kernel level in Windows NT, WMI is also used to manage drivers operating within the Windows Driver Model (WDM). Services also exist to collect data from the 32-bit Windows environment, data from the Registry, from the Performance Monitor and from SNMP and DMI. This data is all consolidated within WMI and then presented via CIM.

Via WMI, Windows-based management applications can use DCOM/COM-based applications to access, monitor, and control devices and applications either as discrete elements or as independent components within the enterprise. These interfaces are accessible for programs and scripts, either directly through its own API set or through ODBC, OLE DB, and ADSI. From non-Windows environments, access to the schema will also be available via popular Web based technologies such as XML, HTML, and ASP.

CIM has become widely supported by third-party vendors as a means of gathering management information via WMI. Microsoft Systems Management Server 2.0 in conjunction with third-party solutions from major players such as BMC Software, Compuware Corporation, Computer Associates International, Hewlett-Packard, and Tivoli Systems have all announced support for CIM on Windows 2000 Server.

As with Windows NT Server 4.0, a Simple Networking Management Protocol (SNMP) monitoring agent is also included, allowing any standardized SNMP management package to monitor machines running Windows 2000 Server.

Management Scripting Services

Windows 2000 Server provides a set of management scripting services in the form of the Windows Script Host (WSH) to automate complex management tasks. This provides several benefits, such as automated responses when administrators are unavailable.

WSH is a language-independent scripting host for ActiveX scripting engines running on 32-bit Windows platforms. WSH allows scripts to be run directly on the desktop or from the command prompt. Both Microsoft VBScript and Microsoft JScript development software are supported as scripting language choices as part of the Windows 2000 operating system. There is also a Perl engine available with the services for UNIX add-on pack. Third parties can also provide ActiveX scripting engines for other popular languages such as TCL, REXX, Python, and others.

Two separate ActiveX interfaces are provided. Administrators can use that object provided by Windows Script Host (WSH) and any ActiveX controls that expose ActiveX automation interfaces to perform various administrative tasks on the Windows platform.

Automation can be provided through defining a scripted action as a result of one or more events occurring, where the script acts on controllable applications either via ActiveX Automation, or indirectly via CIM. In more complex situations, an action may take place as a result of events arriving over time in a specific sequence. Administrators can also use the object interfaces provided by WSH and any ActiveX controls that expose automation interfaces to perform various administrative tasks against the operating system.

Another powerful management scripting feature of Windows 2000 is the net shell (netsh). Net shell provides a command-line interface for configuring routing, remote access, DHCP, WINS and other essential network services. Not only can administrators configure these services, but they can use netsh to create scripts to automate local and remote service management as well. The net shell also features single command configuration save and restore for routing, remote access, DHCP, WINS and other supported services.

Group Policy Services

In Windows 2000 Server, group policies define user and computer settings for groups of users and computers. Administrators can create a specific desktop configuration for a particular group of users and computers with the Group Policy Editor – an MMC snap-in. The Group Policy Settings administrators create are contained in a Group Policy Object (GPO) that is in turn associated with selected Active Directory objects, such as sites, domains, or organizational units.

Administrators can use the Group Policy Editor and its extension to define Group Policy options for managed desktop configurations for computers and users. With the Group Policy Editor, administrators can specify the following settings:

- Software Policies, to mandate registry settings on the desktop, including operating system components and applications.
- Scripts (such as computer startup and shutdown, logon and logoff).
- Software Installation options including lists of available applications for users, and so forth.
- User and Data Settings for file deployment and redirecting special folders.
- Security Settings to configure access restrictions for both the local computer as well as domain and network related options.

When administrators use the Group Policy Editor, they create Group Policy settings that are contained in a Group Policy Object (GPO). These GPOs are in turn associated with selected directory objects (sites, domains, organizational units, etc).

The specifics of the Group Policy infrastructure in Windows 2000 Server can be summarized as follows:

- **Administrative Templates** – The Group Policy Editor requires a source to create the user interface settings an administrator can set. For this purpose, the Group Policy Editor can use either an MMC extension snap-in to the Group Policy Editor snap-in or an ASCII file referred to as an administrative template. The administrative template specifies the registry settings that can be modified through the Software Policies extension of the Group Policy Editor. It consists of a hierarchy of categories and subcategories that together define how the options are displayed through the Group Policy Editor user interface. It also indicates the registry locations where changes should be made if a particular selection is made, specifies any options or restrictions (in values) that are associated with the selection, and in some cases specifies a default value to use if a selection is activated.

- **Group Policy Editor** – The Group Policy Editor is an MMC snap-in that includes built-in features for setting Group Policy. Group policies define the various components of the user's environment that system administrators need to manage and include software settings, application deployment options, scripts, user data and settings options, and security settings.
- **Application Deployment Editor** – The Application Deployment Editor is an MMC snap-in extension of the Group Policy Editor that to centrally manage software distribution. With the Application Deployment Editor, administrators can install, assign, publish, update, repair, and remove software for groups of users and computers.
- **Security Configuration Editor** – The Security Configuration Editor is used by the Group Policy Editor to define security configuration for computers within a Group Policy Object. A security configuration consists of security settings applied to each security area supported for Windows 2000 Professional or Server. This security configuration is included within a GPO and is then applied to computers as part of the Group Policy enforcement. Areas that can be configured via the Security Configuration Editor include the following:
- **Account Policies** – Refers to computer settings for password policy, lockout policy, and Kerberos policy in Windows NT domains.
- **Local Policies** – Includes security settings for Audit policy, user rights assignment, and security options. Local policy allows administrators to configure who has local or network access to the computer and how local events are audited.
- **Event Log** – Controls security settings for the Application, Security, and System event logs. Administrators can access these logs using the Event Viewer.
- **Restricted Groups** – Computer security settings for built-in groups that have certain predefined capabilities. Restricted Group policies affect the memberships of groups such as the built-in local groups including Administrators, Power Users, Print Operators, and Server Operators or global groups such as Domain Administrators.
- **System Services** – Controls configuration settings and security options for system services such as network services, file and print services, telephony and fax services, Internet services, and so forth. The Security Settings extension directly supports general settings for each system service including startup mode and security on that service.
- **Registry** – Used to configure and analyze settings for security descriptors (including object ownership), the Access Control List (ACL), and auditing information for each object (volume, directory, or file) in the local file system.
-
- **Windows Installer Service** – The Windows Installer Service is responsible for managing application installation, modification, repairs, and removal. It includes an operating system-resident install service, a standard format for component management, and a management API for applications and tools. The elements comprising the Windows Installer Service can be summarized as follows:

- **Resident Install Service** – Windows Installer Service is a resident feature of the Windows 2000 operating system. It will also be provided via a redistributable pack for Windows 9x and Windows NT 4.0 platforms. The Windows Installer Service Pack for those platforms will be made available to the developer community for distribution as part of their products. Once installed in the operating system, the Windows Installer Service can process installation requests from Windows installer-enabled applications. Future versions of the Designed for Microsoft Windows Logo Program will standardize on Windows Installer for setup.

- **Component Management Format** – Windows Installer views all applications as being composed of three logical building blocks – products, features, and components. A product corresponds to a single package or SKU. Features refer to parts of a product from the user's perspective. Finally, a component refers to the parts of a product from the developer's perspective. Each Windows installer product is described in the form of a single Windows Installer package file. This file (.msi) is in a database format that has been optimized for installation performance and describes, among other things, the relationships between features, components, and resources for a given product. At installation time, the Windows Installer service opens the package file for the product and determines the installation operations that must be performed to install that product.

- **Management API** – The Windows Installer Service provides management API-enabling tools which allow application developers to programmatically inventory a computer's contents, install and configure Windows Installer products, install and configure Windows Installer features, and determine the path to specific Windows Installer components on the computer. The most key feature of the management API is that it allows the Windows Installer service to manage all file paths on behalf of an application. At runtime, a Windows Installer-installed application can ask the Windows Installer service for the path to a given component. This level of indirection completely frees applications from hard dependency on static file paths.

- **On-Demand Installation of Products** – Windows Installer supports advertisement at the product level. Both the Shell and OLE use the Windows Installer Management API in Windows 2000 Server, therefore allowing an entire product to be advertised. Advertising a product installs only the entry points to it, including desktop and Start menu shortcuts, file extensions, and OLE registration. When a user triggers the activation of the application, the operating system calls Windows Installer to install the necessary features of the advertised product. When the installation is complete, Windows Installer will automatically launch the application for the user.

- **On-Demand Installation from Within Applications** – The on-demand install capability ensures that all application features are available to users – even those that were not previously installed. Instead of requiring users to rerun Setup to add optional components, Windows Installer is automatically called when a user makes a feature request to silently install the optional components.

- **Runtime Resource Resiliency** – The Windows Installer management API enables dynamic repair of an application in much the same way that it enables on-demand installation. When an application calls Windows Installer to resolve a path, Windows Installer performs two checks. The first verifies that the requested component is installed. The second verifies whether or not the component is properly installed (assuming that the first check succeeded). In the case that it is not, an on-demand repair shall be performed, allowing applications to repair itself silently within the course of normal usage.

Management Infrastructure Summary

Windows 2000 Server provides a comprehensive management infrastructure. Its Group Policy services are the most comprehensive. It provides a complete software installation and management service – the Windows Installer Service coupled with the desktop application management services. Additionally, its security configuration manager, policy management services, and application deployment features provide the best directory integration, the easiest configuration tools, and the most comprehensive feature-set. Windows 2000

Server also provides an equally impressive management scripting implementation and the most capable, easiest-to-use management tools with its MMC-based configuration and management tools. Windows 2000 Server provides a complete set of management instrumentation services, which extends to full SNMP support and a complete implementation of the Desktop Management Task Force's Web-Based Enterprise Management protocol in the form of WMI.

Windows NT Server 4.0 provides an excellent set of easy-to-use graphical management tools, although they are not integrated like Windows 2000 and definitely not as easy to use as the MMC snap-ins present in Windows 2000. Some MMC snap-ins are provided for management of certain network services such as Internet Information Server or Transaction Server, enhancing the administrator's experience. Windows NT Server 4.0 also supports both SNMP and the DMTF's WBEM standard with the WMI implementation contained in the Service Pack 4 update. Management scripting services are excellent – providing a solution essentially identical to that found in Windows 2000 Server when the Windows NT Option Pack is installed on Windows NT Server 4.0. However, where Windows NT Server 4.0 really falls short of Windows 2000 Server is in its group policy services implementation. Windows NT Server 4.0 user policy management implementation is not nearly as feature-complete and Windows NT Server 4.0 offers no software package administration equivalent to Windows 2000 Server Windows Installer Service.

Though Solaris 7 does provide fairly efficient management services, these services are not as feature rich or easy to use as either Windows NT 4.0 or Windows 2000 management services. Although graphical administration tools lack the integrated approach of Windows offerings, the command-line is one area where Solaris 7 is strong. The command-line tools available are both versatile and powerful. Yet they are also inherently more complex to use and require more experience to operate (even when compared to Windows command-line counterparts). Solaris 7 provides full support for WBEM and also provides an SDK for developers. The Sun WBEM implementation is Java-based and supports many industry standard technologies including Common Information Model (CIM), Extensible Markup Language (XML), SNMP and Desktop Management Instrumentation (DMI). Finally, user realms provide functions similar to Group Policy. However, user realms aren't as dynamic or configurable as Windows 2000 group policies, making the Windows 2000 Group Policy implementation the clear leader.

Desktop Management

Lowering the total cost of ownership (TCO) of a network operating system is a significant driving factor for the IT departments in many organizations. One of the most efficient ways to reduce TCO is via centralized change and configuration management. In this scenario, administrators have complete control from a central location over the desktops within their organizations. Key functionality that should be present in any feature-complete centralized change and configuration management implementation includes the following:

- **User Data Management Services** to mirror/cache user configuration files and data between their desktop and the server, allowing for enhanced performance and reliability.
- **Desktop Application Management** provides administrators with the ability to deploy software automatically without having to visit PCs. In addition, applications should automatically fix themselves upon corruption or removal of necessary files.
- **Operating System Installation** services should be provided to allow the administrator to automatically deploy operating systems over the network (either via special boot floppies or network boot-capable systems) to eliminate the need for individual desktop visits.
- **User Settings Management** should be provided to allow administers to centrally control and store the user's work environment. The administrator should be able to control what aspects of the operating system a user can access (eliminating unnecessary help desk calls by inexperienced users mistakenly configuring their systems), centrally define preferences such as printer paths, and ensure that a user's environment is

replicated when moving from machine to machine to eliminate the need for constant environmental reconfiguration.

Solaris 7 Implementation Details

For the most part, the desktop management capabilities of Solaris 7 are weak. However, Solaris 7 does support remote operating system installation and remote desktop application management. These features are implemented through Solaris Web Start and the Solaris Web Start API.

With Solaris Web Start, administrators can remotely install the Solaris operating system. With the default installation option, the operating system and all bundled software packages are automatically installed on the remote system. With the custom installation option, administrators can select software to install and configure the Solaris installation. The option to format and configure file systems is also available. Online help can guide inexperienced administrators through the installation process. Finally, secure authentication ensures that only authorized personnel can remotely install the operating system.

The Solaris Web Start Wizards can be used to install and update software remotely using Solaris Web Start technology. When doing so, administrators can use default or custom installation options and must also authenticate themselves prior to execution. Using the associated developer toolkit, third party vendors can add Web Start support to their applications as well.

Windows NT Server 4.0 Implementation Details

Windows NT 4.0 also has weak desktop management capabilities. No user desktop management solution is provided, leaving administrators and clients with no real solution to manage user data files between the local machine and the server. No desktop application management solution is provided with Widows NT Server 4.0 either. However, this functionality is available with Microsoft Systems Management Server.

Change and configuration management on the Windows NT Server 4.0 platform is accomplished with the addition of a freely available add-on – the Zero Administration Kit (ZAK). The ZAK is a set of tools, methodologies, and guidelines for IT managers that incorporates and supplements existing Windows technologies to simplify the implementation of a centralized, policy-based change and configuration management model on the Windows NT 4.0 platform.

At a high level, the ZAK provides the following functionality:

- **Centralized Configuration** – Administrators can specify exactly what business applications the user is allowed to run, the look of the desktop, and where the user data is allowed to reside. This is all managed centrally requiring no visit to the desktop. This helps ensure worker focus and productivity.
- **Elimination of Local Access to the Desktop** – Users are prevented from installing applications on their desktops or making any changes to the system configuration, preventing costly downtime.

It should be noted that ZAK only provides user/desktop settings management functionality. Specifically, ZAK enables administrators to lock down desktops and prevent end user operations that result in help desk calls, eliminate end-user access to system files and features, remove the ability to install unapproved applications, and provide centralized configuration of the desktop. Software distribution is not a feature of ZAK, instead customers have to look to Microsoft Systems Management Server (SMS), which fully integrates and compliments ZAK, for this type of functionality on the Windows NT Server 4.0 platform.

By default, the Zero Administration Kit operates in one of two modes – each one providing varying degrees of control over the user's desktops. These modes can be summarized as follows:

- **TaskStation Mode** is an ideal configuration for a "Tasked Oriented" worker, such as an order entry clerk or bank teller that requires access to a single line of business applications. It provides complete lock down of the desktop. The Windows user interface is disabled, which prevents a user from accessing any additional applications or data including the Start button, the Taskbar, the Task Manager, the Control Panel, and the file system.

- **AppStation Mode** is designed for the typical worker who runs multiple applications but does not need or have the experience to access system configuration options or install other applications. It boots the desktop into an administrator constrained Windows interface, providing users with access to just the business applications that they need. Access is restricted to Task Manager, Control Panel, and the file system.

Additionally, both the TaskStation and AppStation mode can be fully customized to provide a solution that meets the exact needs of the customer. Other desktop management functions are accomplished via the System Policy Editor, which allows all operating system policies and settings to be centrally managed. The storage of user profiles on network servers allows user profiles (and all associated restrictions) to roam with them from workstation to workstation, ensuring that settings and restrictions are maintained between systems. With the ZAK feature-set in conjunction with the Windows NT system policies configured in the System Policy Editor, the administrator has complete, centralized control over the desktop and what users can and cannot do on his network, helping to reduce administrative overhead and lower TCO.

The necessary templates and other infrastructure pieces are also provided to allow administrators to deploy ZAK itself as well as ZAK-enabled versions of the Windows operating system. An automated setup program creates server shares and unattended client installations to ease and automate the deployment of ZAK within an environment

Windows 2000 Server Implementation Details

Windows 2000 Server provides an exceptionally comprehensive desktop management solution – IntelliMirror management technologies. Designed to lower total cost-of-ownership of Windows 2000 Server-based networks, IntelliMirror provides a unique management solution that combines with advantages of centralized computing with the performance and flexibility of distributed computing.

User Data Management

User data management features support mirroring of user data to the network and local caching of selected network data. The following capabilities are supported:

- Data resides locally for offline use.
- Data resides on the server for protection.
- Data is mirrored so that it exists in both the local computer and on the server.
- Data can follow the user if the user moves to another computer.

These capabilities provide the following advantages to the system administrator:

- Increased data protection by using Information Technology-managed backup.
- Increased accessibility so any computer on the network can be used to access data.
- Increased availability means that caching maintains data on the local computer even when it is disconnected from the network.

Desktop Application Management

Windows 2000 Server IntelliMirror management technologies software has been designed to facilitate application installation, updates and repairs, and un-installations in managed environments. System administrators can use the Software Installation and Maintenance features to deploy or upgrade applications in any of the following ways:

- **Advertised Applications** allow administrators to advertise an application during logon at a workstation. When an application is advertised, the shortcuts for the application are added to the appropriate locations (including the Start menu or the desktop), and the appropriate registry entries for the application are added to the local computer registry. The applications administrators assign to computers are automatically installed.
- **Assigned Applications** allow administrators to match applications with users who require them to perform their jobs. For example, if everyone in an organization requires a particular order entry application, administrators can assign that application to everyone – this process assigns the application and makes it available on everyone's desktop.
- Administrators can also assign applications to specific workstations, in which case the application will install automatically the next time the computer is restarted. It should be noted that when an application is assigned to a user, it is actually being advertised by creating shortcuts and updating the registry for such things as file associations. With the advertisement information stored on the local computer, the application itself will be installed when the first request to activate the application occurs, such as the user selecting the icon from the desktop or Start menu or by opening a document associated with the assigned application.
- Additionally, if an administrator assigns a newer version of the application (an upgrade), the upgrade is advertised the next time the user logs on and the upgrade itself is installed the first time the user invokes the application. It should also be noted that when an application is assigned to a workstation instead of a user, it is installed automatically the next time the computer is logged on to the network. Finally, it should also be pointed out that assigned applications are resilient – if a user deletes an assigned application it will automatically be readvertised and reinstalled.
- **Published Applications** allow for applications to be stored as Group Policy Objects associated with users in Active Directory containers. Published applications do not appear to be installed on the local computer; no shortcuts appear on the user's desktop and no registry entries are made in the local computer. Published applications are advertised to Active Directory rather than to the local computer registry. Published applications can be installed in one of two ways – user's can open files associated with the application or select it from a list via the Add/Remove Programs tool in the Windows 2000 control panel.

User Settings Management

IntelliMirror includes functionality that allows administrators to centrally manage user and computer settings. With IntelliMirror, user settings are mirrored to the network, and administrators can define specific computing environments for users and computers including:

- Add new users and computers remotely.
- Define settings for groups of users and computers.
- Apply changes for groups of users.
- Restore user's settings if the user's computer fails.
- Ensure that a user's desktop settings follow the user if he or she moves to another computer.

Similar functionality to the features offered by the ZAK on Windows NT Server 4.0 are also present and integrated into the operating system to allow administrators to lock-down and centrally control a user's desktop configuration to prevent unnecessary help desk calls.

Remote Operating System Installation

In addition to the IntelliMirror feature-set, Windows 2000 Server provides a remote operating system functionality to remote install capable clients from Windows 2000-based servers configured with this feature. The remote installation process installs an operating system on the local computer's hard disk using a remote source (CD image on a server). Normally, a workstation that is participating in the remote installation model is set to boot off of the local disk. However, in remote installation mode, the workstation first boots from the network to get the operating system installed on the local disk. The network boot is initiated either by the BIOS or by a special boot floppy. In either case, the network boot is controlled by boot code that adheres to the Net PC specification. The preferred BIOS boot model for this environment is one in which the BIOS gives the user a small window prior to booting off the disk in which a special key press causes a remote boot and installation off of the network.

In a Net PC-compatible network boot, the boot code uses the Dynamic Host Configuration Protocol (DHCP) and boot information negotiation layer (BINL) to get an IP address for the workstation and find a boot server. The boot code then uses the Trivial File Transfer Protocol (TFTP) to download a boot program from the remote installation server and transfers control to it for operating system installation to commence.

Desktop Management Summary

For customers seeking to reduce TCO via centralized change and configuration management, Windows 2000 Server provides a number of features and capabilities within this realm. It features two-way mirroring/caching of user data between the client and the server, which provides many benefits to the administrator including canalized backup of user data and easier machine replacement. Its software installation and maintenance infrastructure is also the most sophisticated, which supports the publishing of applications – where users can see that a package is available and then choose whether or not to install it. Windows 2000 Server also offers tight directory integration with its software deployment solution, making it easy to administer. Windows 2000 Server enables the centralized management of the user's desktop and features a set of comprehensive management. Finally, the Remote Operating System Installation feature provides many benefits to system administrators seeking to roll out operating systems on managed PCs – a feature that is unmatched by the two other solutions.

Windows NT Server 4.0 provides neither software distribution capabilities nor user data management feature-sets. Instead, with the addition of Zero Administration Kit, the operating system desktop can be centrally controlled and move with the user from computer to computer as part of the operating system's roaming profile support.

The desktop management capabilities of Solaris 7 aren't very extensive. Still, Solaris 7 does support both remote operating system installation and remote desktop application management, making the operating system a better choice than Windows NT 4.0 if you need remote installation capabilities. However, in other areas, such as desktop configuration and controls, Windows NT 4.0 excels and Windows 2000 supports all these features and more.

Security

A secure network operating system has many characteristics. However, as a common ground, security implementations can usually be broken down into authentication, encryption, public key infrastructure, and security management schemes. Specific review criteria for these areas can be identified as follows:

- **Authentication –** Support should extend to the latest Internet standards for network authentication including Kerberos V5 and Transport Layer Security. This is in addition to providing an authentication mechanism that is backward compatible with clients from prior versions of the network operating system. Additionally, smart cards should also be supported for client authentication.

- **Encryption Services –** Beyond authentication, encryption support should also be present in the operating system. Internet services should extend to support the Secure Sockets Layer (SSL) protocol in both standard 40-bit and 128-bit strong encryption strengths. File system encryption should be supported to help secure sensitive data stored on disk.
- **Public Key Infrastructure** – A directory-integrated X.509 Version 3 Certificate server should be provided as part of the operating system. X.509 client certificates should be usable as a means of both network and Web-client authentication.
- **Centralized Security Management** – Services should be provided to allow for centralized administrative control for operating system security policies, allowing administrators to be able to maintain security without having to visit individual systems.

Solaris 7 Implementation Details

Authentication

Solaris 7 supports the Sun Enterprise Authentication Mechanism. Authentication is managed through the Key Distribution Center. The KDC manages account information for users, applications and servers. Central management of authentication through the KDC allows for single login to the enterprise, making it possible for users to access servers, applications and other resources on the network without having to re-enter login information. Administrators can control and manage authentication from a single console.

As with directory information, security information can be replicated between master and slave servers. Replication speeds up the authentication process and provides back copies of the KDC database in case the master fails. Through the use of user realms, administrators can set organizational boundaries for users and systems. Clients can be authenticated between realms as well.

The Sun Enterprise Authentication Mechanism uses Kerberos V5 security and encryption as specified in RFCs 1510 and 1964. Through this authentication mechanism, Solaris supports secure access to NFS, Telnet, FTP and remote commands. The Remote Procedure Call API (RPCSEC_GSS) allows third-party vendors to create secure applications for Solaris as well. The RPCSEC_GSS security protocol is specified in RFC 2203.

Encryption

Beyond Kerberos V5 authentication and encryption, Solaris 7 supports a number of encryption options. With remote users and VPN, Sun Screen SKIP supports 40-bit RC2, 40-bit RC4, 56-bit DES CBC, 128-bit RC4, 128-bit SAFER CBC and 3-key Triple-DES encryption.

Secure Sockets Layer (SSL) encryption at the standard 40-bit encryption strength and 128-bit Strong SSL is currently provided as well. Using SSL, sensitive information can be encrypted for Web-based clients accessing information on Solaris 7 servers via the HTTP protocol. WebNFS, SMTP, and other mails services also support SSL for encryption.

Public Key Infrastructure

PKI Services provides a complete X.509 Version 3 certificate. With this, X.509v3 certificates can be securely issued to either employees or business partners. The PKI Services implementation also provides integration with external Certificate Authorities to have certificates signed by trusted commercial providers. With remote access and VPNs, Simple Key-management for Internet Protocols is used. SKIP supports shared keys, public keys, and X.509 v3 certificates. Certificates are supported through the Sun Certificate Manager, which must be installed for certain SSL functions, such as secure communications in the directory.

Several key technologies are used to support the public key infrastructure. Diffie-Hellman key exchange is used for automatic key distribution whereby SunScreen SKIP can securely distribute keys. SKIP uses a private and public key to create public key certificates for users. The public certificate is then exchanged between hosts. A technology, called Certificate Discovery, allows Solaris systems running SKIP to retrieve certificates from other computers running SKIP.

Centralized Security Management

Solaris with Easy Access Server doesn’t provide centralized security management. However, tools are provided to manage specific aspects of security. For example, certificates are managed through Sun Certificate Manager and authentication is managed through the Sun Enterprise Authentication console.

Other Encryption Features

Solaris 7 supports other industry standard encryption features, including Transport Layer Security (TLS), smart cards and file system encryption. Of particular interest are smart cards. Smart cards provide tamper-resistant storage for protecting private keys, account numbers, passwords, and other forms of personal information. This enables portability of credentials and other private information between computers at work, home, or on the road. Smart Cards also eliminate the need to transmit sensitive information, such as authentication tickets and private keys, over networks.

Windows NT Server 4.0 Implementation Details

Authentication

As with prior versions of Windows NT Server, LAN Manager encrypted authentication continues to be used for network logon. This provides a clean, secure method of gaining access to the network and maintains 100 percent compatibility with all Microsoft-compatible network clients currently in the hands of customers.

Encryption

Microsoft Internet Information Server 4.0 provides complete support for the SSL protocol. This allows for both 40-bit and 128-bit strong encryption for Internet communications via the HTTP, SMTP, and NNTP services implementations present in IIS 4.0.

Public Key Infrastructure

Windows NT Server 4.0 provides some public-key capabilities with the inclusion of Microsoft Certificate Server in the Windows NT Option Pack. Certificate Server provides an X.509 Version 3 certificate services implementation, allowing certificates to be securely issued to employees and business partners without the need to rely on an external Certificate Authority. Complete integration with IIS 4.0 is provided, allowing certificates to be issued via the Web and to be used as a means of secure client authentication over the Internet.

Centralized Security Management

Included with Service Pack 4 for Windows NT Server 4.0 is the Security Configuration Editor (SCE). SCE provides automated configuration of various global and local security settings access controls on files and registry keys, and security configuration of system services – all via a friendly graphical user interface. Additionally, it allows administrators to define security configurations as a template and then apply the template to selected computers in one operation.

Windows 2000 Server Implementation Details

Authentication

Windows 2000 Server provides two new authentication options – Kerberos Version 5 and Transport Layer Security (TLS) – in addition to the LAN Manager authentication support in Windows NT Server 4.0. Kerberos is a mature, industry-standard network authentication protocol. On Windows 2000 Server, it can provide fast, single login to Windows 2000 Server-based enterprise resources, as well as to other environments that support this protocol such as several varieties of UNIX. Kerberos-based authentication provides additional benefits such as mutual authentication and delegated authentication. Mutual authentication provides a stronger level of assurance because both the client and the server must prove their identities to each other. Delegated authentication is particularly useful in multi-tier environments because it enables a user's credentials to be tracked through the entire end-to-end transaction. TLS provides additional Internet standards-based authentication support.

Windows 2000 Server also introduces smart card support on the Windows platform. With its smart card infrastructure, Windows 2000 can use smart cards for network logon and authentication. Additionally, policies can be set so that specific users will be required to use smart cards to gain access to the network.

Public Key Infrastructure

A comprehensive public key infrastructure is an integrated feature of Microsoft Windows 2000 Server. At the core of this implementation is Certificate Services, which provides an Active Directory-integrated X.509 Version 3 certificate server. With Certificate Services, users of Windows 2000 can securely issue certificates to their employees and business partners without the need to use a third-party Certification Authority. Additionally, Windows 2000 Server can use certificates issued by commercial Certificate Authorities.

With the advent of TLS authentication in Windows 2000 Server, certificates can be used as a means of operating system authentication. External users who do not have Windows NT accounts can be authenticated using public-key certificates, which are mapped to an existing user account. Access rights defined for this user account determine the resources the external users can use to access the system. Client authentication using public-key certificates also allows Windows 2000 Server to authenticate external users based on certificates issued by trusted Certificate Authorities. Cross-root certification can also be configured to allow for integration between internally issued public-key certificates and externally issued certificates from commercial Certificate Authorities.

As with Windows NT Server 4.0, complete integration between Certificate Services and Internet Information Services is provided. This allows for certificates to be deployed through a Web-based interface and provides the capability for internally issued certificates for secure Web authentication.

Beyond client authentication, public key security has several prominent uses within the Windows 2000 operating system. Certificate Services is tightly integrated with Internet Information Services, allowing for secure Web applications to be easily deployed on Windows 2000 Server. Additionally, digital signatures can be used within Windows 2000 Server to assure the authenticity of objects (such as software components or e-mail messages).

One of the other features of the public key infrastructure in Windows 2000 Server is the introduction of the CryptoAPI. This provides an easy-to-program certificate management API set to provide for the rapid development of applications to deploy and manage public key certificates. Additionally, many easy-to-use tools and common interface dialogs for managing the private key/public-key pairs and the associated certificates have been provided to ensure that management of the public key services is an easy task for system administrators. Storage of personal security credentials, which uses secure disk-based storage, is easily transported with Microsoft's proposed industry-standard protocol, Personal Information Exchange.

Other Encryption Features

Beyond the public key infrastructure, Windows 2000 Server provides several encryption implementations within the operating system including:

- **Encrypting File System (EFS)**, which provides protection for the storage of sensitive data on the NTFS file system. This file-level encryption uses cryptography with the existing access control model on NTFS to provide a new level of protection for data stored on disk. The encryption technology utilizes a combination of public key technologies for key management and symmetric cryptographic algorithms for data encryption. EFS runs as an integrated system service, making it easy to manage, difficult to attack, and transparent to the user. It provides the key management technology allowing an enterprise to designate data recovery agents to enable business-driven data recovery needs. When encrypted files are backed up to tape, they remain in an encrypted form, resulting in better protection of data on tape backups.
- **SSL Support in Internet Information Services** provides both 40-bit and 128-bit strong encryption support for HTTP, SMTP, and NNTP services, providing for the secure transmission of information over the Internet.

Centralized Security Management

The Security Configuration Editor (SCE) tool is carried over from Windows NT Server 4.0 and enhanced in Windows 2000 Server. It adds policy based security management and configuration with the Active Directory service, providing a complete centralized, directory-enabled security management tool for Windows 2000 Server customers.

Security Summary

Windows 2000 Server provides a sophisticated security infrastructure. At the authentication level, it provides Internet-standards based authentication, supporting Kerberos and Transport Layer Security. It also provides integrated smart card support. In terms of public key infrastructure services, Windows 2000 Server features the ability to use public key certificates for client authentication and an extensible API set for developing public-key based applications. Its X.509 certificate services implementation is also the most complete and features the best directory integration. Finally, Windows 2000 Server offers encryption support within the file system to secure sensitive data.

Windows NT Server 4.0 falls behind Windows 2000 Server in this area. It provides none of the advanced authentication options or PKI infrastructure. However, it does feature an excellent X.509 certificate server and excellent encryption support for Internet services. Additionally, with the advent of the Security Configuration Editor in Service Pack 4, Windows NT Server 4.0 features an excellent centralized administration tool to set security policies and then apply them to other servers, greatly easing administrative tasks.

The Solaris 7 product provides a feature-complete implementation of security tools. Support is available for Kerberos V5, TLS, smart cards, X.509 Certificate Servers, 40 and 128-bit SSL and some centralized security management when integrated with Sun Directory Services or NIS+. Still, there is no single tool or location that allows the administration of all aspects of security management.