AUSPEX NETSERVICES

DELIVERING "NO-COMPROMISE" CONSOLIDATION OF UNIX AND WINDOWS NT DATA

Mike Clark and
Greg Govatos

Technical Report 19
March 1998

Executive Summary

While UNIX continues to dominate the back end, enterprise environments are evolving to include NT as a complementary workstation and server platform. Thus, the requirement to integrate NT seamlessly into the enterprise has assumed a critical position. Combining NT and UNIX environments poses a very important data services challenge: Do you separate distributed data servers for NT data or consolidate both types of data on a single platform? Significant benefits in the areas of performance, data management, availability and file sharing, can be obtained by consolidating UNIX and NT data on a single, enterprise-class file server platform.

Deploying each of the available options for consolidating UNIX and NT data [such as NFS client for NT/95 and Microsoft Common Internet File System (CIFS) emulation software, which includes Samba and Syntax TotalNET Advanced Server (TAS)] requires a range of compromises in the areas of performance, NT integration, administration, and support. Taken together, these issues limit the ability of existing products to supporting *small-scale* deployment of NT/95 systems into UNIX-centric environments.

NeTservices™ is the premier solution for deploying enterprise-level shared file services for mixed UNIX and NT/95 environments. With NeTservices, both UNIX and NT data can be managed on the same Auspex NetServer file server, reducing costs and simplifying management while allowing secure, flexible file sharing among UNIX and NT/95 users.

NeTservices delivers an optimized implementation of CIFS protocols that leverages Auspex's proven FMP® architecture to provide industry-leading performance and scalability. High performance and the scalable operation of NFS protocols, which allow file access by UNIX clients, is supported concurrently with CIFS.

NeTservices delivers the NT 4.0 networking environment, including directory services, file security, and remote administration, that is essential for enterprise-level deployment of NT-based networks. Furthermore, it delivers a best-of-breed administrative environment that fully supports NT Server Tools, such as User Manager, Server Manager, and Event Viewer for viewing NT logs.

NeTservices is an Auspex-developed product. It is sold and supported by Auspex. As such, it takes advantage of Auspex's premier pre- and post-sales support organizations, which provide experienced support for enterprise-level file services deployment.

Document #: 300-TC051, Ver. 4.0

Auspex Systems, Inc.
2300 Central Expressway
Santa Clara, California 95050 USA
Phone: (408)566-2000 · Fax: (408) 566-2020
http://www.auspex.com

Table of Contents

INTRODUCTION

Auspex's NetServer 7000 family of enterprise Network File System (NFS) servers delivers unprecedented levels of performance and reliability. They easily scale to support from 40 to more than 800 users running demanding, business-critical applications. The NetServer family provides a field-measured uptime level of 99.989%, which translates to approximately an hour of unplanned downtime in a full year of continuous operation.

The Auspex NetServer employs Functional Multiprocessing (FMP) ®, a patented architecture that addresses the special requirements placed upon network servers today. FMP distributes the data services workload to multiple, dedicated processors individually optimized for network, storage and UNIX operating system functions. The result is an architecture in which UNIX is removed from the NFS I/O data path, yielding gains in both performance and reliability.

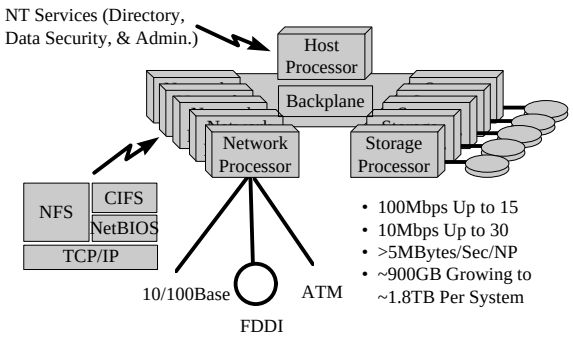


Figure 1 Functional Multiprocessing

At the heart of the NetServer FMP architecture is Auspex's Functional Multiprocessing Kernel (FMK®), a small, fast, message-passing microkernel that delivers high data throughput without intervention from UNIX on the host processor. By circumventing the operating system, I/O requests are serviced more efficiently and reliably, accelerating file operations and freeing host processor cycles for administrative tasks.

NeTservices is a Windows NT Server 4.0-compatible implementation of networking and administrative services for Auspex NetServer 7000 systems (Figure 1). It allows NetServer 7000 systems to concurrently deliver native file services to hundreds of UNIX and NT/95 clients, while being fully integrated into both environments from user access and administrative standpoints.

Based on Microsoft Windows NT 4.0, NeTservices is fully compatible with Microsoft's Common Internet File System (CIFS) file sharing protocol and NT Server 4.0 directory, data security, and remote administration services. No additional software is required on Windows NT, 95, 3.11 and 3.1 clients. NeTservices provides full support for NT domain and trust relationships. Administration from NT clients is also supported.

This paper is intended for IT professionals and system administrators. It describes how the features and benefits of NeTservices address the data services requirements of mixed UNIX and NT/95 enterprise network environments. It includes a discussion of NeTservices performance, support of NT authentication and file security, administration, backup, and capabilities for file sharing among UNIX and NT users. Finally, it includes a brief functional comparison between NeTservices and Windows NT Server 4.0 in these feature areas: core server features, administration, enterprise support, security, and networking.

The paper assumes familiarity with the benefits of deploying Auspex NetServer[1] systems and technical features of such servers. It also assumes familiarity with NT administrative, file services, and networking concepts. For readers unfamiliar with Windows NT networking, a comparative overview related to UNIX networking is provided in Appendix A: UNIX vs. NT Networking. Appendix B: Glossary contains definitions for important terms used in this paper. Appendix C: Additional References section contains a list of books that offer more in-depth information on Windows NT.

1 DATA SERVICES CHALLENGES FOR MIXED NT AND UNIX ENVIRONMENTS

Today's business technology environment is not an "*either* NT *or* UNIX" world—it is *both*. It is not uncommon to see NT and UNIX as the file and application servers platform, in the same enterprise.

Microsoft Windows is the de facto standard operating environment for the desktop. As companies network their Windows desktop systems, the natural choice for the workgroup server platform is rapidly becoming Windows NT. Windows NT provides a familiar interface and improved network, security, and management facilities. Market data clearly indicates that NT is very successful as a commercial server, providing a variety of print and file sharing services for departmental or workgroup applications.

At the same time, market forecasts indicate that Fortune 500 companies plan continued growth in their deployment of UNIX systems. UNIX servers are seen as delivering the requisite degree of performance, high availability, and scalability for deploying enterprise-level application and data services. File servers for UNIX environments are typically required to have these attributes in order to support enterprise-wide file sharing for business-critical functions. Additionally, data consolidation has occurred on UNIX file servers, so users can easily collaborate on projects such as financial services, CAD, and software development.

While UNIX continues to dominate the back end, these environments are evolving to include NT as a complementary workstation platform. Some will evolve entirely to NT, while others will stop at some mixture of these systems. Regardless of where the enterprise is headed, the fact remains that when the first NT box is brought in, a way is needed to integrate it seamlessly into the enterprise.

BENEFITS OF CONSOLIDATING UNIX AND NT DATA

Combining UNIX and NT environments poses a very important data services challenge: having separate, distributed data servers for NT data versus consolidating both types of data on a single platform. There are several benefits that can be obtained by consolidating UNIX and NT data on a single, enterprise-class file server platform, including:

- *Performance Scalability*

  Delivering data over the network is a I/O throughput issue, not a CPU performance issue. The architecture of standard Intel SMP servers is not geared to address I/O throughput, so minimal file services performance increase is seen by adding more CPUs to a PC file server.

- *Central Data Management*

[1] A range of overview and technical product information is available, including *An Overview of NFS Service Using Functional Multiprocessing*, Technical Report 10, Auspex Systems, Inc. March, 1997.

*I*s the corporate IT staff going to grow as the number of servers to manage grows? If not, deploying additional servers will cause the burden to grow.

- *High Availability*

  With NT, server availability is typically measured in terms of 98.XX% uptime while UNIX uptime is typically measured in terms of 99.9X%. While the differences may not be striking in percentage terms, they certainly are in hard-number terms. *98% uptime equals 200 hours of outage per year, while 99.9% uptime equals 10 hours of outage per year*.

- *File Sharing*

  In many high-intensity collaborative environments such as engineering, software development, documentation, and financial trading, there is one *logical* copy of data that needs to be accessed and updated by multiple users running UNIX and NT/95 desktops. Deploying separate UNIX and NT file servers limits the ability to share data (unless a cumbersome data replication scheme is put place), and results in multiple physical copies.

CHALLENGES OF UNIX AND NT DATA CONSOLIDATION[1]

A number of options are available for consolidating UNIX and NT data, including NFS client software for NT/95 desktops, Samba CIFS emulation software for a range of UNIX operating systems, and Syntax's TotalNET Advanced Server (TAS) for Sun Solaris and other operating systems. Although the benefits of such consolidation are clear and quantifiable, deploying each of these options requires a range of compromises in performance, NT integration, administration, and support. Taken together, these compromises invalidate the benefits of consolidating UNIX and NT data.

- *Performance*

  Most CIFS implementations for UNIX servers, such as Samba and TAS, deliver *emulated* implementations (running as user-level processes and not run in the UNIX kernel) of the CIFS file services protocol, resulting in relatively low performance. These emulated file services are typically appropriate for only casual CIFS file access. For example, emulated CIFS files services are appropriate in a high-intensity UNIX environment where users infrequently access CIFS file services for Office Automation (OA) applications.

- *NT Integration*

  Existing products, including CIFS products for UNIX and NFS packages for NT/95, provide minimal integration with NT networking services, such as domain directory services, file/directory security services, and remote administration services, that are essential for deploying NT in corporate environments. This limits such products to supporting small-scale deployment of NT/95 clients.

- *Administration*

  Deploying NFS client packages for NT/95 requires significant overhead of per-client installation and on-going administration. CIFS packages for UNIX servers typically provide unconventional administrative interfaces that are unfamiliar to NT administrators. Administration of NT user accounts and data security policies either requires use of manual editing of UNIX-based configuration files or proprietary graphical user interfaces (GUIs). Both of these options are inconsistent with corporate NT administrative policies which require use of standard NT Server Tools, such as Server Manager, User

[1] "Appendix A: NT versus UNIX Networking Services" presents helpful background information for this section.

Manager, and Event Viewer, for managing NT user accounts, data security, and file services properties.

- *Support*

  Lack of reliable support is a prevalent issue with existing UNIX/NT data consolidation solutions, as these packages are sold by third parties to run as add-ons to volume UNIX server platforms. Software vendors delivering such products have minimal experience in supporting large-scale, corporate-level file services deployment.

Overall, the above issues limit the fitness of existing products to supporting *small-scale* deployment of NT/95 systems into UNIX-centric environments. And, until the introduction of NeTservices, the goal of enterprise-class shared file services for UNIX and NT environments as an IT infrastructure component remained illusory.

2 NETSERVICES OVERVIEW

NeTservices was developed to deliver enterprise-class file services allowing data consolidation and file sharing in a mixed UNIX and NT/95 environment. It provides the following benefits:

- *Enterprise-level Consolidation for UNIX and NT/95 data*

  With NeTservices, both UNIX and NT data can be managed on the same Auspex server, reducing costs, and simplifying management. Further, customers can now obtain very high levels of data availability for both UNIX *and* NT data as the NetServer 7000 platform has been field-measured to deliver in the range of *1 hour* of service interruption *per year*.

- *Secure, flexible file sharing among UNIX and NT/95 users*

  NeTservices allows customers to manage only one physical copy of the shared data. It provides features allowing transparent, yet secure sharing of individual files by UNIX and NT clients. Further, it provides support for mechanisms allowing data protection in place of concurrent file access by UNIX and NT clients.

- *High-performance, Native Shared File Service*

  NeTservices delivers an optimized implementation of CIFS protocols that leverages the proven FMP architecture to provide industry-leading performance and scalability. High-performance and scalable operation of NFS protocols, allowing file access by UNIX clients, is supported concurrently with CIFS.

- *NT 4.0 Networking Environment*

  NeTservices delivers the NT 4.0 networking environment, including directory services, file security and remote administration, which are essential for enterprise-level deployment of NT-based networks.

- *NT Remote Administration*

  NeTservices does not require overhead of per-client administration. Further, it delivers a best-of-breed administrative environment that fully supports NT Server Tools such as User Manager for user account administration, Server Manager for managing NT server properties, and Event Viewer for viewing NT logs.

- *Enterprise-level Support*

  NeTservices is an Auspex-developed product. It is sold and supported by Auspex. As such, it will take advantage of Auspex's pre- and post-sales support organizations experienced in supporting enterprise-level file services deployment.

3 NETSERVICES PERFORMANCE

In order to support the overall goal of enterprise-level consolidation of UNIX and NT data, NeTservices delivers an FMK-based, optimized implementation of the CIFS file services protocol providing very high NT file services performance. The Auspex CIFS implementation is expected to deliver up to near-linear CIFS performance scalability as additional Network Processor sub-systems are added to the server system. The largest configuration consisting of CIFS concurrently running on 5 Network Processors is expected to exceed the sequential CIFS performance provided by multiple NT file server systems.

A key requirement for support of enterprise-level shared file services is for the data consolidation platform to concurrently deliver NFS and CIFS file services with undiminished performance and scalability. The Auspex CIFS implementation allows individual Network Processors to concurrently run while the NetServer system simultaneously delivers NFS and CIFS protocols with sustained performance and scalability.

Comparative performance benchmark information using network activity profiles of high-intensity environments, such as CAD, financial services, and software development, is in the process of being collected and will be published as it becomes available.

4 SECURITY UNDER NETSERVICES

NT DOMAIN SECURITY

The NT domain security model provides single logon capability for NT networks. An NT *Domain* is defined as a group of servers running Windows NT Server that share common security policies and *user*/*group* account databases. Therefore, the Windows NT Domain is the basic unit of security and centralized administration for Windows NT clients and servers in the domain, which in some ways, can be viewed as a single system.

One server running Windows NT Server acts as the Primary Domain Controller (PDC), which maintains the centralized security databases for the domain. Other computers running Windows NT Server in the domain function as Backup Domain Controllers (BDC) and can authenticate logon requests. Users of a Windows NT Domain are authenticated by the PDC or BDC. Changes in security policies are implemented on the PDC and transparently replicated to BDCs.

Another key concept in Windows NT Domains is the Trust Relationship. A trust relationship is a link between two domains that enables a user with an account in one domain to have access to resources, such as files and directories, in another domain.

NeTservices provides full support for the NT Domain security model including support for PDC, and BDC, mode of operation. NeTservices support of the NT Domain security model also includes the capability to respond to validation requests from users/groups in *trusted domains* and support of authentication of *local* and *global groups.*

NT ACCESS CONTROL LISTS

Windows/NT uses a set of standard Access Control Lists (ACLs) for granting access to shares[1], directories, and files. The ACLs offer useful combinations of specific types of access, which are called individual permissions. Individual permissions are somewhat analogous to UNIX permissions. They consist of: Read (R), Write (W), Execute (X), Delete (D), Change Permissions (P), and Take Ownership (O). UNIX supports three sets of file and directory permissions: owner, group, and world. This is the familiar -rwxrwxrwx that shows up in the output from the UNIX **ls -al** command.

With Windows NT, permissions can be granted to either individual users or to groups. The major difference between Windows NT and UNIX is that in Windows NT each user or group can be granted its own set of permissions for each file and/or directory. This allows a finer degree of access control and therefore greater flexibility. In UNIX assignment of access control is effectively limited to 3 entities, the owner of the file/directory, the primary group, and the rest of the world.

NeTservices includes full support for both share-level and file/directory-level permissions. Management of such permissions can be accomplished by authorized administrators using Windows NT/95/3.11 Explorer, Server Manager, or File Manager GUI tools.

5 NETSERVICES ADMINISTRATION

NeTservices supports a best-of-breed administration environment for NT services and data. NT administrators can autonomously administer all NT services, such as file-sharing, user account, and file security, running on NetServer 7000 systems. In addition, enterprise-class solutions running on Auspex servers that deliver high-performance and robust storage management for UNIX data can be leveraged for NT data.

Windows NT administration is based on a client/server model utilizing Windows NT Remote Procedure Call (NT RPC) technology. This is a decentralized model, which dramatically simplifies many of the tasks usually associated with system administration. The Windows NT Server 4.0 administrative environment, which is fully integrated with its Windows-based, graphical user interface (GUI), includes the following tools:

- User Manager for Domains provides the same function as the UNIX method of manually edit the **/etc/passwd** and **/etc/groups** files such as adding, modifying, renaming users/groups, and managing security policies.
- With auditing enabled, Event Viewer can be used to monitor system events such as such as when a particular user last logged on to the domain.
- Server Manager is the NT GUI tool for monitoring and managing server properties, such as who is connected to a server, how long they have been connected, and what resources they have open. It can also be used for management functions such as closing open resources, and disconnecting users connected to a share.

NeTservices provides full support for NT 4.0 tools for remote administration, including User Manager, Event Viewer, and Server Manager. This support is enabled by the inclusion of a full implementation of

[1] Shares on NT servers are directories that are accessible to NT/95 network users using browsing interfaces such as Network Neighborhood or File Manager GUIs. *Share-level permissions* control access to all of the files and subdirectories within the share. NT *file and directory permissions* must be used if it is required to restrict access to parts of the shared directory tree.

NT RPC in NeTservices. Finally, centralized UNIX-based data management, for tasks such as managing disk storage, RAID, and backup, is fully supported for NT data.

6 FILE SHARING USING NETSERVICES

Support of transparent sharing of individual files among UNIX and NT/95 users is a key goal behind the delivery of the NeTservices product. Each filesystem on a NetServer running NeTservices can support one of the following three file-sharing modes:

- NFS-only—only authorized NFS clients can access and share files in the filesystem.
- CIFS-only—only authorized CIFS clients can access and share files in the filesystem.
- NFS/CIFS mixed-mode—both types of authorized clients can access and share files in the filesystem.

A number of value-added facilities in the locking and file-sharing areas are provided that enable secure and robust high-performance sharing of files among UNIX and NT/95 users.

FILE LOCKING

NeTservices includes support for PC-style *mandatory* file/record locking that is fully compatible with NT/CIFS file/record locking. The goal behind such mandatory locking functionality is to allow robust access by multiple authorized NT/95 clients to the same file or record. CIFS locking is the only locking mechanism used by clients when accessing CIFS-only filesystems. NFS Lock Manager (*lockd*) will continue to be supported as the advisory locking mechanism used by clients when accessing NFS-only filesystems.

COORDINATED LOCKING

The need for sharing individual files by UNIX and NT users is primarily driven by the emergence of UNIX and NT versions of specific applications supporting a common, interchangeable file format. Mixed-mode NFS/CIFS filesystems that can be shared across UNIX and NT/95 clients enables such file sharing in a robust fashion. NeTservices has been designed to support two alternative means for coordinated, “safe” (that is, file data is fully protected against corruption) access by UNIX and NT/95 clients to individual files.

1. NeTservices provides an optional facility that allows CIFS locking to be enforced with respect to NFS accesses so that NT/95 clients are fully protected against concurrent NFS accesses to the same file. Specifically, each mixed-mode filesystem can be configured so that all NFS accesses to a file that is locked by CIFS clients are blocked.
2. NeTservices is fully compatible with high-level application-based locking. This refers to applications[1] using Relational Database Management Systems (RDBMS) or shadow files to support locking information. NeTservices is designed to allow interoperation with such applications.

A future release of NeTservices will support server-based coordination between NFS and CIFS locking to allow coordinated access across UNIX and NT/95 clients. This is to support safe, coordinated access to data by multiplatform applications using platform-specific locking, such as NFS Lock Manager and CIFS

[1] Examples include MCAD applications such as ProEngineer, EDS/Unigraphics and CoCreate that use Product Data Managers (PDMs), and Frame’s use of shadow files to manage locked file access across UNIX and NT/95 clients.

file/record locking (versus applications using built-in locking functionality to provide coordinated access as in alternative 2. above).

FILE ACCESS CONTROL

Automatic coordination between the UNIX and NT file access control mechanisms is critical if file sharing across UNIX and NT clients is to be supported in a flexible and secure fashion.
NeTservices provides mechanisms that allow UNIX file permissions to automatically work with NTFS permissions to allow secure file sharing among UNIX and NT/95 clients with a minimum of administrative overhead. Figure 2 shows the sequence of file access permission tests applied in mixed-mode operation. Specifically, NT ACLs (which are set by using NT Server Manager, File Manager, or Explorer tools) function as the first level of file security for access by NT/95 users to files in mixed-mode filesystems. UNIX file/directory permissions are used as the second level of file security for file accesses by NT/95 users. This is accomplished through an optional mechanism allowing mapping of NT domain-based user/group accounts to UNIX user accounts. (Note that logon validation for NT users/groups continues to be provided by NT PDC/BDC servers). UNIX permissions continue to be the means for managing file security for UNIX users.

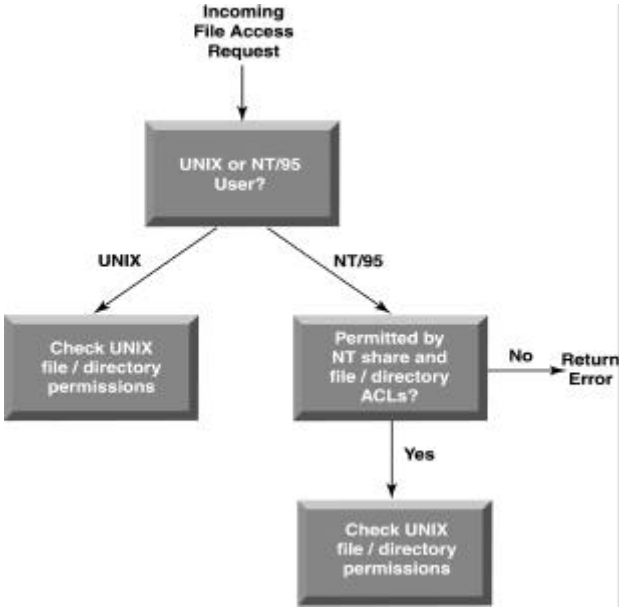


Figure 2 File Access Control

7 BACKUP SERVICES

Auspex NetServer 7000 systems support a range of third-party, UNIX-based backup tools, including products from Legato, Intelliguard and OpenVision. NeTservices allows NT data to be backed up using these UNIX-based, enterprise-level backup products.

Auspex NetServer software also provides a specialized interface, the Auspex FastBackup interface, that moves data directly from disk to tape, using only the Storage Processor in the modular FMP architecture. FastBackup-enabled products from OpenVision and Intelliguard can also be used for higher-performance backups of NT data on Auspex servers.

8 FUNCTIONAL COMPARISON OF NETSERVICES AND WINDOWS NT SERVER 4.0

NeTservices allows NetServer 7000 systems to concurrently deliver *native* file services to hundreds of UNIX and NT/95 clients, without compromising on support of native file access performance, security, and administration capabilities of UNIX and NT environments. The tables below compare NeTservices with Microsoft's Windows NT Server 4.0 in a number of important feature areas. Please refer to the *Glossary* for more information on terms used in these feature comparisons.

- *Core Server Features*

  All main NT 4.0 core server features are supported in the first release of NeTservices except Print Services.

- *Administration Features*

  All pertinent Windows NT 4.0 remote administration features are supported.

- *Enterprise Support Features*

  All pertinent Windows NT 4.0 directory services features for resource access across a global, domain-based network are supported.

- *Security Features*

  NeTservices includes a full implementation of the NT 4.0 security model. It includes support for DES method of encryption for changing of passwords and replicating user/group account information. The optional RC4 encryption is not supported.

- *Networking Features*

  NeTservices supports TCP/IP, the most widely used transport protocol in the computer industry. Support for the following Windows NT 4.0 transport protocols is not provided: NetBEUI (which is more suitable for small networks as it cannot be forwarded over routers) and NWLink (the Microsoft-developed protocol compatible with Novell's IPX/SPX protocol).

Core Server Features	**Windows NT Server 4.0**	**NeTservices**
File Services for all current Microsoft Clients (Windows NT/95/3.11/3.1, DOS)	Yes	Yes
Print Services for all Microsoft Clients	Yes	No
Enhanced Windows NT User and Administrative Client Interoperability including NT Client Validation/Access Control	Yes	Yes
Participation in network as Primary Domain Controller	Yes	Yes
Participation in network as Backup Domain Controller	Yes	Yes

Administration Features	**Windows NT Server 4.0**	**NeTservices**
Administration from Windows NT/Windows 3.1/3.11 clients	Yes	Yes
Administration from NT/95 Clients (via User/Server/Explorer tools)	Yes	Yes
Administration from local server console via command line interface (NET commands)	Yes	Yes

Enterprise Support Features	Windows NT Server 4.0	NeTservices
Simplified Enterprise Support via server participation in multi-domain Trust Relationships	Yes	Yes
Mixed case filename support	Yes	Yes
Support of NT-style local/global groups	Yes	Yes

Security Features	Windows NT Server 4.0	NeTservices
Full Support for NT Security Model including user-resource Security ID's (SIDs)/ discretionary NTFS Directory and File Access Controls/ Security Account Manager (SAM)	Yes	Yes
Full Support for NT Style Auditing/ Error Logging and Viewing via NT Event Viewer	Yes	Yes
DES Encryption	Yes	Yes
RC4 Encryption	Yes	No
Account Lockout	Yes	Yes

Networking Features	Windows NT Server 4.0	NeTservices
Transports Supported	TCP/IP, NetBEUI, NWlink	TCP/IP
Wide-area Services	Yes-WINS	Yes-WINS

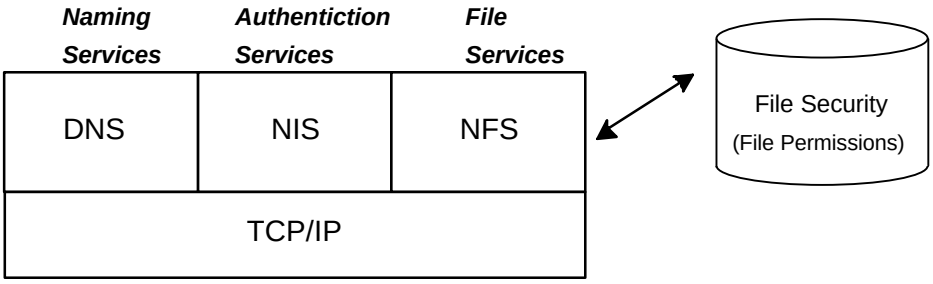
9 CONCLUSION

NeTservices is the premier solution for deploying enterprise-level, shared file services for mixed UNIX and NT/95 environments. It allows Auspex NetServer 7000 systems to provide data consolidation and file-sharing for such environments without compromising support of native file access performance, NT integration, and NT remote administration capabilities.

NeTservices supports an implementation of Microsoft native CIFS file sharing protocol that leverages the proven FMP architecture to provide industry-leading performance and scalability. Furthermore, it delivers the NT 4.0 networking environment including directory services, file security, and remote administration, that is essential for deploying NT in corporate environments. Finally, NeTservices delivers a best-of-breed administrative environment that fully supports remote NT administrative tools for user/group account and file server properties management as well as enterprise-level administration tools for managing disk storage, RAID, and backup/restore.

APPENDIX A: NT VS UNIX NETWORKING SERVICES

The native functions between Windows NT and UNIX services are not very different. UNIX users are familiar with the following networking architecture.



UNIX Networking Services

Figure 3 UNIX Networking Services

Naming Services: Domain Name Service (DNS) is a hierarchical name service for TCP/IP hosts that is the standard IP address resolution method in UNIX environments. DNS domains should not be confused with Windows NT *domains.*

Authentication Services: The database of user authentication information (usernames, group affiliation, and password) is typically maintained by NIS (Network Information Service) in UNIX environments or in **/etc/passwd** configuration files on a per-server basis.

File Services: NFS, originally developed by Sun Microsystems, allows directories and files to be shared across a network. It is the de facto UNIX standard for network file systems and has been ported to many non-UNIX operating systems as well. Through NFS, users and software can access files located on remote systems as if they were local files.

File Access Security: UNIX supports three sets of file and directory permissions: owner, group and world. This is the familiar **-rwxrwxrwx** that shows up in the output from the UNIX **ls -al** command.

Not surprisingly, the Windows NT network architecture looks very similar, as shown below.

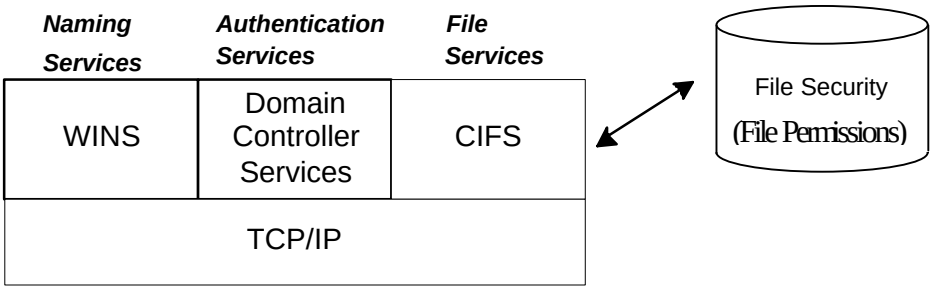


Figure 4 NT Networking Services

The services perform similar functions, including:

- *Naming Services*

The Windows Internet Name Service (WINS) provides a dynamic database for registering and querying name-to-IP address mappings in an NT network environment. NT systems can also be configured to use DNS for communication with non-Microsoft systems in the local or wide-area network. Although DNS might seem similar to WINS, there is a major difference: DNS requires static configuration for computer name-to-IP address mapping, while WINS is dynamic and requires less administration.

- *Authentication Services*

  Users/groups of a Windows NT Domain are authenticated by the Primary or Backup Domain Controller (PDC/BDC) for the domain. Trust relationships between two domains enables users/groups with accounts in one domain to securely access resources in another domain. This allows secure sharing of resources, such as files, servers, and printers, across the enterprise network.

- *File Services*

  Windows NT provides a built-in network file system through its Common Internet File System (CIFS, formerly called Server Message Block of SMB) redirector and server components. CIFS is the latest dialect of the X/Open standard SMB protocol. CIFS is based on the SMB dialect known as Windows NT LAN Manager (NT LM) 0.12--the SMB protocol with special calls that duplicate Windows NT semantics. SMB was first introduced by Microsoft in the early '80s and is the protocol used in several diverse PC network environments: Windows95, Windows for Workgroups and LAN Manager.

- *File Access Security*

  Windows NT offers a set of standard Access Control Lists (ACLs) or permissions for share, files and directory access by users and groups. These standard permissions offer useful combinations of specific types of access, which are called individual permissions. Individual permissions consist of: Read (R), Write (W), Execute (X), Delete (D), Change Permissions (P) and Take Ownership (O).

With Windows NT, permissions can be granted to either individual users or to groups. The big difference between Windows NT and UNIX is that, with Windows NT each user or group can be granted their own set of permissions for each file and/or directory. This allows a finer degree of access control and therefore greater flexibility. With UNIX, you are effectively limited to assigning access control to 3 entities, the owner of the file/directory, the primary group, and the rest of the world.

APPENDIX B: GLOSSARY

access right	The permission granted to a process to manipulate a particular object in a particular way (for example, by calling a service). Different object types support different access rights.
audit policy	Defines the type of security events that are logged for a domain or for an individual computer; determines what Windows NT will do when the security log becomes full.
auditing	The ability to detect and record security-related events, particularly any attempts to create, access, or delete objects. Windows NT uses Security IDs (SIDs) to record which process performed the action.
domain	For Windows NT Server, a networked set of workstations and servers that share a Security Accounts Manager (SAM) database and that can be administered as a group. A user with an account in a particular network domain can log onto and access his or her account from any system in the domain. See also *SAM database*.
domain controller	For a Windows NT Server domain, the servers that authenticate domain logons and maintains the security policy and the master database for a domain. Both *primary* and *backup* domain controllers are capable of validating a user's logon; however, password changes must be made by contacting the primary domain controller.
domain database	See *SAM database*.
domain name	The name by which a Windows NT domain is known to the network.
event	Any significant occurrence in the system or in an application that requires users to be notified or an entry to be added to a log.
Event Log service	Records events in the system, security and application logs.
global user account	For Windows NT Server, a normal user account in a user's home domain. If there are multiple domains in the network, it is best if each user in the network has only one user account, in only one domain and each user's access to other domains is accomplished through the establishment of domain trust relationships.
group	An account containing other accounts called members. The permissions and rights granted to a group are also provided to its members, making groups a convenient way to grant common capabilities to collections of user accounts. *Global groups* created in one domain can also be granted privileges in domains that trust the host domain. *Local groups* can be assigned privileges only in the domain in which they were created. Local groups can contain user accounts and global groups whereas global groups can only contain user accounts.
logon authentication	Refers to the validation of a user either locally or in a domain. At logon time, the user specifies his or her name, password and the

	intended logon *domain*. The workstation then contacts the *domain controllers* for the domain which verify the user's logon credentials.
NetBEUI transport	NetBIOS (Network Basic Input/Output System) Extended User Interface. One of the local area network transport protocols in Windows NT, in addition to TCP/IP and IPX/SPX.
NetBIOS interface	A programming interface that allows I/O requests to be sent to and received from a remote computer. It hides the specifics of networking hardware for applications.
NTFS (Windows NT file system)	A file system designed for use specifically with the Windows NT operating system. It supports object-oriented applications by treating all files as objects with user-defined and system-defined attributes such as access control lists.
partition	A portion of a physical disk that functions as though it were a physically separate unit.
permission	A rule associated with an object (usually a directory, file, or printer) in order to regulate which users can have access to the object and in what manner. See also *right*.
right	Authorizes a user to perform certain actions on the system. Rights apply to the system as a whole and are different from *permissions*, which apply to specific objects. (Sometimes called a *privilege*.)
SAM	See *Security Accounts Manager*.
SAM database	The database of security information that includes user account names and passwords and the settings of the security policies.
Security Accounts Manager	A Windows NT protected subsystem that maintains the SAM database and provides an API for accessing the database.
security ID (SID)	A unique name that identifies a logged-on user to the security system of Windows NT. A security ID can identify either an individual user or a group of users.
system default profile	For Windows NT Server, the user profile that is loaded when Windows NT is running and no user is logged on. When the Welcome dialog box is visible, the system default profile is loaded. See also *user profile*.
trust relationship	Trust relationships are links between domains that enable pass-through authentication, in which a user has only one user account in one domain, yet can access the entire network. A *trusting* domain honors the logon of a *trusted* domain.
user account	Consists of all the information that defines a user to Windows NT. This includes the username and password required for the user to log on, the groups in which the user account has membership and the rights and permissions the user has for using the system and accessing its resources. See also *group*.
user profile	Configuration information retained on a user-by-user basis. The information includes all the per-user settings of Windows NT, such as

	the desktop arrangement, personal program groups and the program items in those groups, screen colors, screen savers, network connections, printer connections, mouse settings, window size and position and more. When a user logs on, the user's profile is loaded and the user's environment in Windows NT is configured according to that profile.
user right	See *right*.
username	A unique name identifying a user account to Windows NT. An account's username cannot be identical to any other group name or username of its own domain or workstation. See also *user account*.
validation	Authorization check of a user's logon information. When a user logs on to an account on a Windows NT workstation computer, the authentication is performed by that workstation. When a user logs on to an account on a Windows NT server domain, that authentication may be performed by any server of that domain. See also *trust relationship*.
WINS	See *Windows Internet Name Service*.
Windows Internet Name Service	A dynamic database for registering and querying NetBIOS name-to-IP address mappings in a routed network environment. WINS consists of two components: WINS clients and servers. When network resources are requested (for example, while browsing the Network Neighborhood, looking for CIFS shares) the WINS client receives the most current information from the WINS server about other hostnames' IP addresses. If these remote machines should be rebooted with new addresses, the WINS server will be notified and its address maps updated automatically.

APPENDIX C: ADDITIONAL REFERENCES

Microsoft Press publishes a range of books for the entire family of Microsoft products about Windows NT. They range from introductory tutorials to books about the internals of Windows NT and cover most audiences along the way.

Here are several useful titles:

- *Microsoft Windows NT 4.0 Step by Step*
- *Running Windows NT 4.0*
- *Windows NT 4.0 Guidelines for Security, Audit, and Control*
- *Inside Windows NT 4.0*
- *Inside the Windows NT File System*
- *Advanced Windows NT 4.0*

The *Windows NT Resource Kit*, published by Microsoft Press, is the definitive source of technical information about Windows NT. It consists of the following four books and associated software:

- Volume 1: *Windows NT Resource Guide*
- Volume 2: *Windows NT Networking Guide*
- Volume 3: *Windows NT Messages*
- Volume 4: *Optimizing Windows NT*