MARCH 1994

NOVELL® RESEARCH

Providing DOS and MS Windows Users with Access to UNIX/NFS Files

Mala Ranganathan
Technical Marketing Manager
USG Marketing

This Application Note profiles two methodologies to provide DOS and MS Windows users with transparent access to UNIX/NFS file systems. One method is to install NFS client software at the personal computer level. The other method is to use an NFS Gateway at the server level. This AppNote will explain the advantages and disadvantages of each approach.

Trademarks

Novell, the N-Design, and NetWare are registered trademarks, and AppWare, AppWare Bus, AppWare Foundation, AppWare Loadable Module, ALM, and Visual AppBuilder are trademarks of Novell, Inc. Tuxedo, UNIX, and UnixWare are registered trademarks of UNIX System Laboratories, Inc., a wholly owned subsidiary of Novell, Inc.

Macintosh is a registered trademark of Apple Computer, Inc. IBM and OS/2 are registered trademarks of International Business Machines Corp. MS-DOS and Windows NT are trademarks of Microsoft Corporation. All other product names mentioned are trademarks of their respective companies or distributors.

Disclaimer

Novell, Inc. makes no representations or warranties with respect to the contents or use of these Application Notes (AppNotes) or of any of the third-party products discussed in the AppNotes. Novell reserves the right to revise these AppNotes and to make changes in their content at any time, without obligation to notify any person or entity of such revisions or changes. These AppNotes do not constitute an endorsement of the third-party product or products that were tested. Configuration(s) tested or described may or may not be the only available solution. Any test is not a determination of product quality or correctness, nor does it ensure compliance with any federal, state, or local requirements. Novell does not warranty products except as stated in applicable Novell product warranties or license agreements.

Novell, Inc.
122 East 1700 South
Provo, Utah 84606 USA

Contents

Introduction

Recent years have seen a growing trend toward incorporating UNIX systems into business environments that were traditionally dominated by PCs. The purpose of this Application Note is to profile two methodologies for DOS and MS Windows users to access UNIX/NFS file systems, so you or your customers can choose the product/method that best suit your needs. This AppNote will discuss the two methods and the advantages and disadvantages of each.

Why Desktop PC Users Need to Access UNIX Files

In this era of multiplatform networks, PC users require access to UNIX systems for a variety of reasons, including the following:

The Prevalence of PC-LAN Environments

The Prevalence of PC-LAN Environments. In the last decade, desktop applications for PCs such as word processors, spreadsheets, databases, and CAD have conquered the corporate world. However, it's no longer sufficient to provide PC users with access to data solely from servers in their own PC-LAN worlds. Business pressures and productivity requirements demand that these users gain access to data and resources on corporate networks.

The Growth of UNIX Environments

The Growth of UNIX Environments. UNIX has recently become more popular in mainstream business. Advances in graphical user interfaces (GUIs) that shield nontechnical users from UNIX commands, the availability of cross-platform applications and steep decreases in UNIX system prices are making UNIX an attractive alternative to many computer users. UNIX systems are used for developing applications and storing mission-critical data.

Integration of PC-LAN and UNIX Environments

Integration of PC-LAN and UNIX Environments. The use of PCs in corporate settings and the growth of UNIX systems into this environment have created a need to integrate the two. The Network File System (NFS), a distributed file-sharing system developed by Sun Microsystems, Inc., is one of the key technologies used in uniting PC LAN and UNIX environments. NFS uses User Datagram Protocol/Internet Protocol (UDP/IP) as its underlying transport protocol and is virtually platform independent (UDP is part of the TCP/IP protocol suite). It runs on mainframes, minicomputers, RISC-based workstations, diskless workstations, and PCs.

NFS makes it possible for users to transparently share UNIX-based data using industry-standard protocols.

Many vendors today offer PC-based NFS client products that integrate the PC LAN and UNIX environments and provide transparent NFS/UNIX file sharing. In addition, Novell offers a product that provides integration from a centralized server. A few of the current product offerings are listed in Figure 1.

Note: PC-NFS is a registered trademark of Sun Microsystems and refers specifically to Sun's product. (PC)NFS is a generic term that was decided upon by X/Open.

Figure 1: A sampling of PC-based NFS client products.

Vendor Name	Product Name
Beame & Whiteside	BW-NFS
Frontier Technologies	Super-NFS
FTP Software	PC/TCP for DOS
Helios Software	PCShare

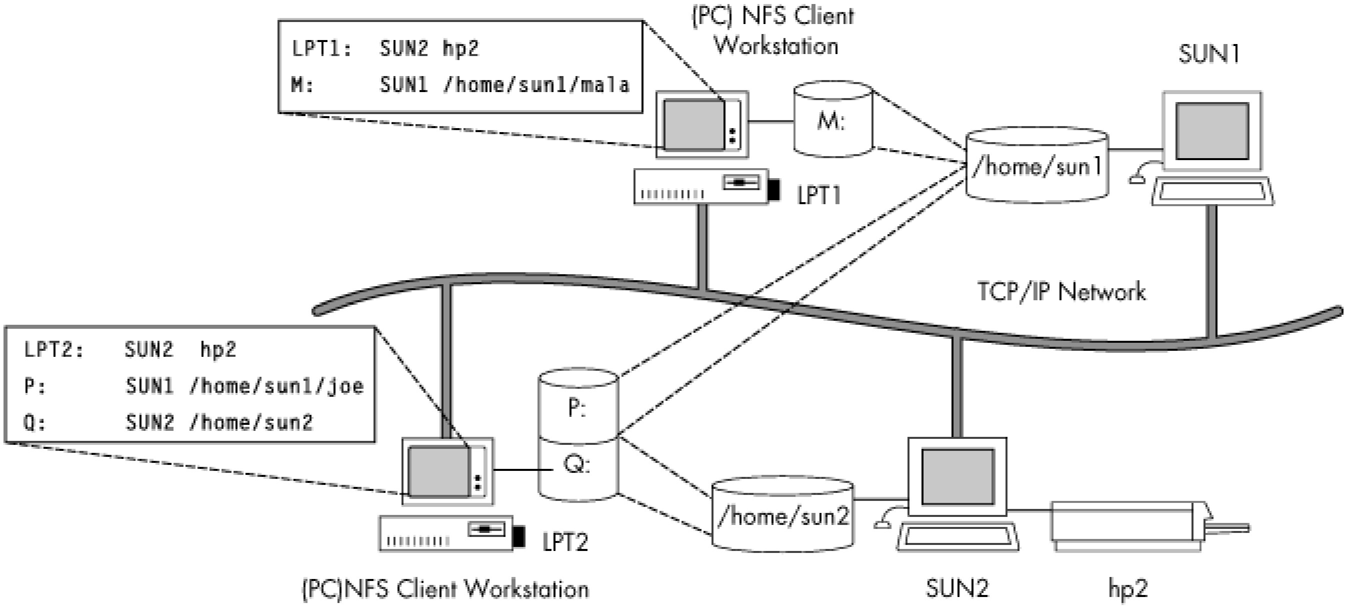
NetManage	ChameleonNFS
Novell	NFS Client for LAN WorkPlace and NetWare NFS Gateway
Sun Microsystems	PC-NFS
The Wollongong Group	PathWay Client NFS for DOS

This AppNote discusses the following methods: installing NFS client software on each PC; installing NFS gateway software on a NetWare server, enabling users to map drives to the NFS system.

Method 1: Installing NFS Client Software on the PC

(PC)NFS client software connects DOS and MS Windows users to NFS servers across TCP/IP networks, as shown in Figure 2.

Figure 2: Method 1 connects PC users to NFS servers across TCP/IP networks.



Method 1 allows users to "link" virtual DOS drives to UNIX/NFS file systems, gaining access to NFS files and printers. The software is installed and configured on each PC. The PC communicates with remote NFS servers by sending NFS requests over TCP/IP using the NFS protocol.

Advantages of the (PC)NFS Method

The (PC)NFS method has the following advantages:

Direct Access to UNIX/NFS Servers. PC users can access any remote NFS server directly, without going through an intermediary system or gateway. Each NFS request is sent directly over the wire to the remote NFS server, which responds to the request. But the response time depends on network traffic and how busy the remote NFS server is.

Scalability

Scalability. (PC)NFS client solutions scale to the limits of the NFS server capacity. You can add more (PC)NFS clients (accessing the same remote NFS server) until the remote NFS server can no longer handle the NFS requests coming from the various (PC)NFS clients. (By the same token, if several high-performance clients send NFS requests to a slow remote NFS server, dropped packets and retransmissions will result.)

Localized Failure

Localized Failure. If the (PC)NFS client software or the PC itself fails for some reason, only the user on that PC is affected. The user can then go to a different PC to resume work until the system is repaired. Other PC users can continue to access the NFS file systems.

Access to Remote UNIX Printers

Access to Remote UNIX Printers. (PC)NFS users can take advantage of UNIX printers on the NFS network by redirecting DOS printer ports (LPT1:, LPT2:, etc.) to UNIX print queues as defined in the /etc/printcap files on the UNIX systems. (PC)NFS clients can send print jobs to the UNIX networked printers.

Popular User Interface

Popular User Interface. Most (PC)NFS implementations today are fully integrated with MS Windows 3.1. Users can access UNIX network resources from their familiar MS-DOS or MS Windows desktops. They can use pull-down menus to connect to network drives and printers from their PCs.

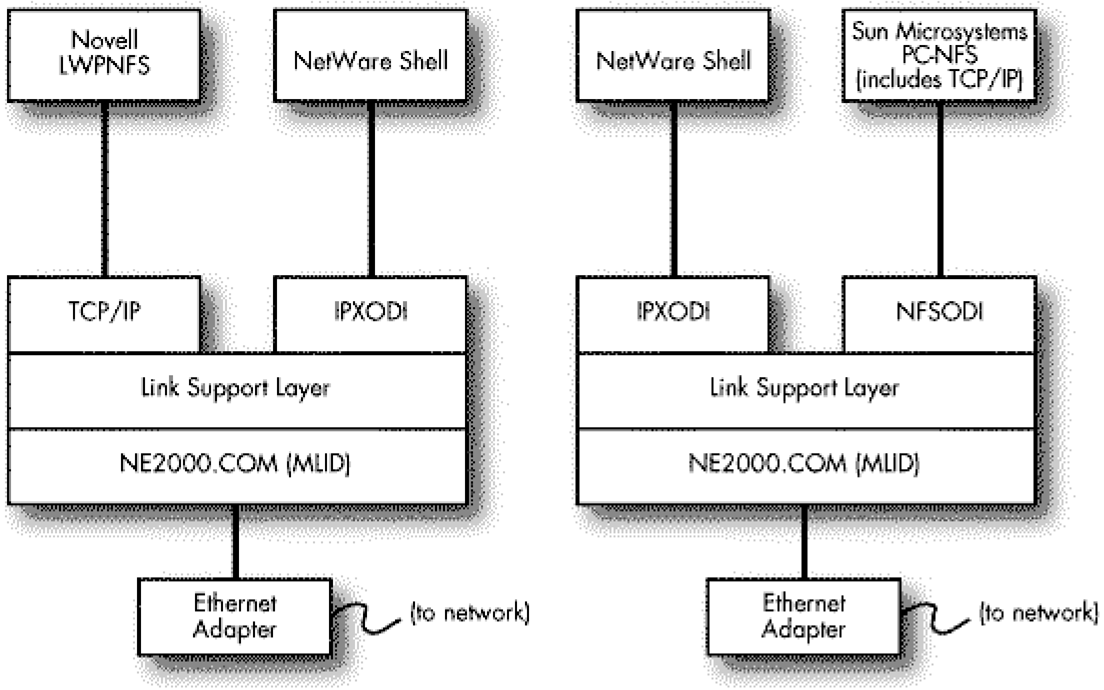
Disadvantages of the (PC)NFS Method

Disadvantages of this method are as follows:

Loading of Multiple Protocols

Loading of Multiple Protocols. You need to load both TCP/IP and IPX/SPX stacks at the (PC)NFS client in order to obtain concurrent access to NetWare and NFS file systems using Open Data-Link Interface (ODI) and/or Network Device Interface Specification (NDIS) drivers. Loading multiple protocol stacks in a PC results in reduced CPU time and available memory for user applications.

Figure 3: Method 1 requires the loading of multiple protocols.



Memory Burden on Client PCs

Memory Burden on Client PCs. The (PC)NFS software can take up a sizeable chunk of conventional memory when loaded on a PC. Some device drivers can be loaded into the system or upper memory to conserve conventional memory. The following two listings detail conventional memory used by PC-NFS (from Sun Microsystems) and LWPNFS (from Novell):

PC-NFS use of conventional memory (using NDIS drivers):

Name	Size in Decimal	Size in Hex
------------	---------------	------------
IBMDOS	16896 (16.5K)	4200
HIMEM	1072 (1.0K)	430
EMM386	4256 (4.2K)	10A0
PCNFS	70736 (69.1K)	11450
SOCKDRV	1344 (1.3K)	540
PROTMAN	96 (0.1K)	60
NE2000	21168 (20.7K)	52B0
NFS-NDIS	7504 (7.3K)	1D50
COMMAND	3392 (3.3K)	D40
PRT	4672 (4.6K)	1240
NET	50640 (49.5K)	C5D0
FREE	64 (0.1K)	40
FREE	288 (0.3K)	120
FREE	472896 (461.8K)	73740
Total FREE =	473248 (462.2K)	

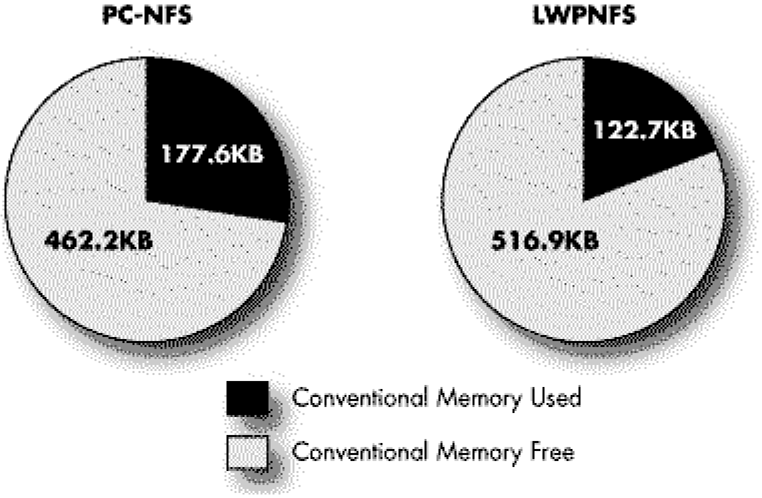
Largest executable program size: 472896 (461.8k)

LWPNFS use of conventional memory (using ODI drivers):

Name	Size in Decimal	Size in Hex
------------	-----------------	------------
IBMDOS	16896 (16.5K)	4200

```
HIMEM                    1072   (   1.0K)            430
EMM386                   4256   (   4.2K)            10A0
ETHDEV                   11968   (  11.7K)           2EC0
COMMAND                  3392   (   3.3K)            D40
LWPRPC                   11120   (  10.9K)           2B70
LSL                      22432   (  21.9k)           57A0
NE2000                   5248   (   5.1K)            1480
TCPIP                     23264   (  22.7K)          5AE0
LWPNFS                   26032   (  25.4K)           65B0
FREE                     64   (   0.1K)              40
FREE                     529280   ( 516.9K)          81380
Total FREE =             529344   ( 516.9k)
Largest executable program size:  529008   (516.6K)
```

Figure 4: PC-NFS and LWPNFS memory requirements.



The following two listings detail conventional memory used by PC-NFS and LWPNFS to load both TCP/IP and NetWare. Again, some device drivers can be loaded into the system or upper memory to conserve conventional memory. Please note that the NETX NetWare shell is loaded rather than the newer VLMs.

PC-NFS use of conventional RAM w/NetWare (ODI drivers):

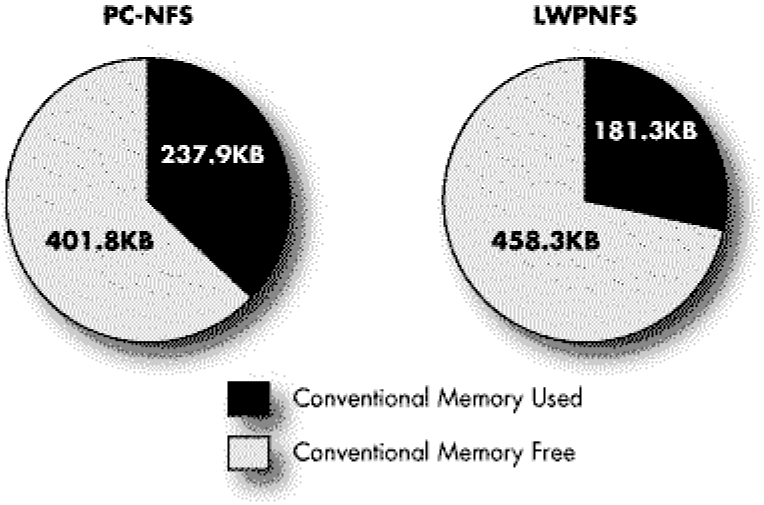
```
Name                     Size in Decimal             Size in Hex
------------             ---------------             ------------
IBMDOS                   16896   (  16.5K)           4200
HIMEM                    1072   (   1.0K)            430
EMM386                   4256   (   4.2K)            10A0
PCNFS                    70736   (  69.1K)           11450
SOCKDRV                  1344   (   1.3K)            540
NFSODI                   2880   (   2.8K)            B40
COMMAND                  3392   (   3.3K)            D40
LSL                      22432   (  21.9K)           57A0
NE2000                   5348   (   5.1K)            1400
PRT                      4672   (   4.6K)            1240
NET                      50640   (  49.5K)           C5D0
IPXODI                   16304   (  15.9K)           3FB0
NETX                     4728   (  42.7K)            AAD0
FREE                     64   (   0.1K)              40
FREE                     304   (   0.3K)             130
FREE                     411024   ( 401.4K)          64590
```

```
Total FREE =                 411392   ( 401.8k)
Largest executable program size:  411024  (401.4K)
```

LWPNFS use of conventional RAM w/NetWare (ODI drivers):

```
Name                         Size in Decimal              Size in Hex
------------                 -----------------            ------------
IBMDOS                       16896   (  16.5K)            4200
HIMEM                        1072   (   1.0K)             430
EMM386                       4256   (   4.2K)             10A0
ETHDEV                       11968   (  11.7K)            2EC0
COMMAND                      3392   (   3.3K)             D40
LWPRPC                       11120   (  10.9K)            2B70
LSL                          22432   (  21.9k)            57A0
NE2000                       5248   (   5.1K)             1480
IPXODI                       16304   (  15.9K)            3FB0
NETX                         43728   (  42.7K)            AAD0
TCPIP                        23264   (  22.7K)            5AE0
LWPNFS                       26032   (  25.4K)            65B0
FREE                         64   (   0.1K)               40
FREE                         469216   ( 458.2K)           728E0
Total FREE =                 469280   ( 458.3K)
Largest executable program size:  468928   (457.9K)
```

Figure 5: PC-NFS and LWPNFS memory requirements when loading both TCP/IP and IPX/SPX.



New Training Required

New Training Required. NetWare users must learn new networking software in order to access the remote NFS file systems. For example, they have to learn new commands and utilities in order to link drives to remote NFS systems.

Software Installation/Configuration on Every PC. The system administrator must install (PC)NFS client software on each DOS client. The LAN board and driver have to be configured with correct information on interrupt, I/O address, and unique IP address. This can be very time consuming for a system administrator. Network drives have to be explicitly linked to the exported NFS file systems on each PC. The network administrator cannot control which remote NFS file system on the NFS network each PC is mounting.

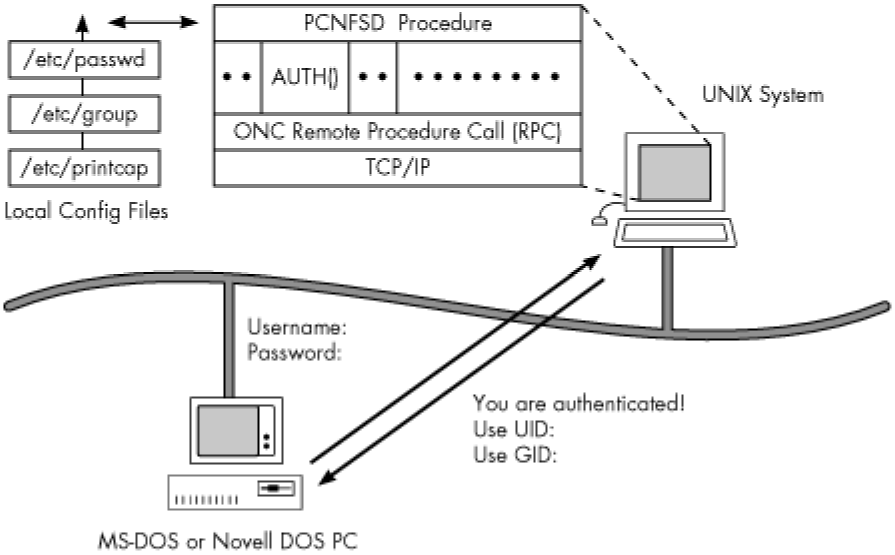
Client-Based Authentication Security Risks. NFS security is built within the client piece of the code, and client-based authentication is not secure by its very definition. The NFS server "trusts" the UID and GIDs in the NFS requests and grants access to the file systems accordingly. It does not perform security checking by itself. It is up to the NFS client software to perform user authentication.

UNIX/NFS Security. When users log in to a UNIX system, they typically quote a username and a password in order to gain access to the system. Once this aspect of security is successfully negotiated, UNIX then views the user as a number called a User ID (UID) and a member of a group called Group ID (GID). In the NFS protocol, these UIDs and GIDs are passed between different machines on an NFS network when the user of a client system attempts to access server files. The NFS server "trusts" that the UID comes from a secure environment (such as another UNIX system) and performs all subsequent security checks using this UID and GID.

(PC)NFS Security. The NFS security breaks down when a DOS client, which has no concept of user identification, is introduced into an NFS network. DOS clients do not force users to authenticate themselves. However, (PC)NFS users need a valid UID and GID to perform various NFS file operations. Most (PC)NFS implementations do not allow PC users to use any UID they choose for NFS server access. Instead, a (PC)NFS authentication server/daemon is used, which typically runs in a "secure" (UNIX system) environment.

The (PC)NFS daemon is a small program (installed on the UNIX system) that offers print spooling and user authentication to PCs running (PC)NFS. It gives UIDs and GIDs to (PC)NFS client systems that quote valid usernames and passwords.

Figure 6: Authentication in a (PC)NFS environment.



The following (PC)NFS daemons are now available:

- PCNFSD, which is provided in source code form by Sun Microsystems. It is a collection of 14 remote procedure calls (RPCs) providing authentication services, print spooling services, printer control, UID <-> Username and GID <-> Groupname mappings. PCNFSD is used by Sun Microsystems' PC-NFS implementation and by other (PC)NFS implementations as well.
- LWPNFSD, which is provided in source code form by Novell. It is a collection of 12 RPCs providing authentication services, print spooling services, printer control, DOS file and record locking services,

UID <-> Username and GID <-> Groupname mappings. LWPNFSD is used by Novell's NFS Client for LAN WorkPlace implementation and by other vendors.

An authenticated user in a (PC)NFS environment has access to NFS file systems on the NFS network, as if he or she were logged in at the UNIX workstation where the authentication daemon runs. If a DOS user has not authenticated against a (PC)NFS daemon, he or she is mapped to UNIX (unprivileged) user "nobody" with a UID of (-2) and GID of (-2). If an NFS file system is not exported with root option, the root user is mapped to nobody with a UID of (-2), which prevents root access on UNIX workstations from spreading across the network.

When a user is authenticated and given a UID and a GID, the NFS client code from most commercial (PC)NFS packages performs some amount of encryption of UID and GID in memory. PC users can bypass the authentication by writing their own NFS client code. A PC user can hunt through the code in the memory and change the UID/GID given by the authentication daemon and use the modified values in subsequent NFS requests, thereby achieving the desired access to NFS file systems on various NFS servers.

The authentication daemon may authorize access to the host on which it is executing, or it may serve a list of specific NFS servers or all the NFS hosts on the network. In the last case, once (PC)NFS users authenticate against the daemon by quoting a valid username/password, the UID/GID(s) returned are used in subsequent NFS requests to all NFS servers. Client-based authentication offers no control over PC users who choose to circumvent the security system.

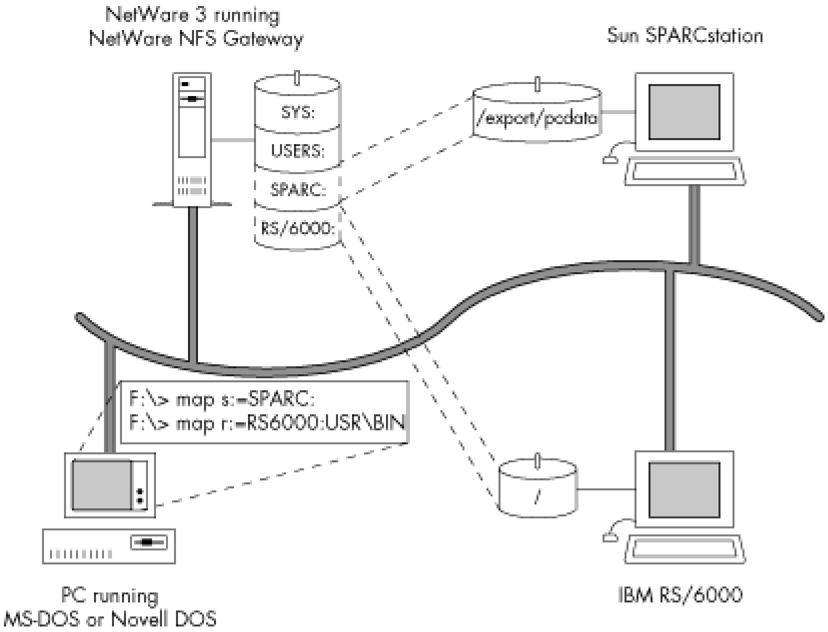
As a hypothetical example, let's assume that (PC)NFS users are to authenticate with an authentication server running in a secure corporate UNIX environment. This allows them to access business-critical data residing in the NFS servers on the corporate backbone. The (PC)NFS users might have root privileges in their local UNIX system but not on the corporate UNIX system. They can modify the user account in the /etc/passwd file or in the NIS map and authenticate as anybody they wish to be against the authentication daemon running in the "unsecure" local UNIX system. They can then access the business-critical data on the network at will.

Method 2: Installing Gateway Software on a NetWare Server

The NetWare NFS Gateway provides DOS and MS Windows users in a NetWare environment transparent access to UNIX/NFS file systems. The NetWare NFS Gateway communicates with NFS servers by sending NFS requests over UDP/IP on behalf of its NetWare client users. The NFS file systems are mounted as "virtual" NetWare volumes.

NetWare client PCs send NetWare Core Protocol (NCP) requests to the NetWare server. The NFS Gateway software intercepts the NCP requests that are not meant for the NetWare server, translates them into NFS requests, and sends them to the remote NFS servers. In this way, DOS and MS Windows users can access NFS file systems without leaving their familiar NetWare environment.

Figure 7: Method 2 is a NetWare server-based solution that offers transparent access to NFS file systems.



```
F:\> map s:=SPARC:
F:\> map r:=RS6000:USR\BIN
```

The NetWare NFS Gateway software is installed on a NetWare 3 server. No changes to the NetWare workstation or the NFS server software are required.

Advantages of the Server-Based Method

Advantages of the server-based method are the following:

Server-Based Solution in a NetWare Environment. The NetWare NFS Gateway is centrally installed on a NetWare 3 server, which eliminates the need to install NFS client software at each workstation.

The NetWare NFS Gateway comes in 5-, 10-, 20-, 50-, 100-, 250-user versions, similar to NetWare 3.11. While NetWare restricts the number of concurrent users logged into the server, the NFS Gateway restricts the number of NetWare users mapped to UNIX/NFS accounts who can access NFS file systems. The NFS-to-NetWare user mapping comes from the NIS (Network Information Services) map for NFSUSERS. The user mapping can be found in the /etc/NFSUSERS file with the corresponding UNIX user entries in the /etc/passwd file, when local files are used. System users whose User ID (UID) value is less than 20 are not included in this user count.

Ability to Use Existing Protocol Stack. NetWare DOS and MS Windows clients do not require a TCP/IP protocol stack in order to access NFS file systems. The IPX/SPX stack used by NetWare workstations will suffice. The NFS Gateway gives NetWare users access to the same files and data that have been traditionally available only to UNIX users via NFS. NFS file systems on various NFS servers appear as NetWare volumes. NetWare users can map drives to those volumes and still use their familiar DOS and NetWare commands and utilities, such as COPY, FILER, and NDIR, etc. NetWare users can access NetWare file and print services as well as NFS file systems.

Reduced DOS Memory Requirements. The NFS Gateway software runs on a NetWare 3 server rather than on each (PC)NFS client. Since this approach doesn't load more networking software in the NetWare client PC's memory, more PC memory is available for applications.

Device Sharing. The NetWare NFS Gateway gives NetWare users access to on-line peripherals such as CD-ROMs and optical jukeboxes available through corporate UNIX machines via NFS.

Centralized Administration. The NetWare NFS Gateway centralizes all management functions. Individual workstations do not have to be configured separately. The NetWare NFS Gateway uses local files and shared databases found in the DNS (Domain Name System) and NIS servers for the IP addresses of all the network NFS servers as well as the NFS user/group information on those servers.

With the DNS/NIS client and server support in the NetWare NFS Gateway, changes to the databases are made at a single location. The hosts database can be maintained in a single host (DNS server) and accessed from any NetWare NFS Gateway on the network. NetWare-to-UNIX mappings of users and groups (which govern NFS file system access) are done at the NIS server if it supports the NFSUSERS and NFSGROUP (NIS) maps. If not, the local NetWare NFS Gateway server maintains these mappings in the /etc/nfsusers and /etc/nfsgroup files.

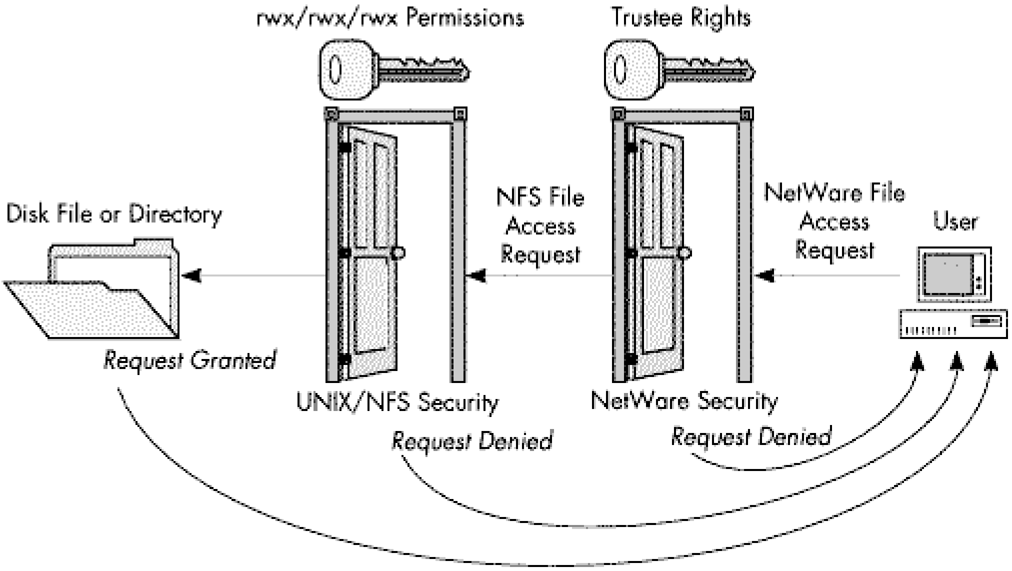
The NFS Gateway centralizes the configuration and the mounting of NFS file systems that remote NFS servers export. After the NFS Gateway mounts the remote NFS file systems, all NetWare workstation users logged in to the NFS Gateway can access the file systems. Their access is subject to NetWare access control rights on the NetWare side and UNIX permissions for files and directories being accessed on the NFS side.

Unlike the (PC)NFS method, the NetWare NFS Gateway gives a network administrator complete control (from a centralized location) of user access to specific NFS file systems. In contrast, (PC)NFS users link their drives to remote NFS file systems independent of each other. Each PC can have drives linked to its own set of NFS file systems, making it difficult for a network administrator to manage the network.

NetWare and UNIX Security Enforced. In order to access UNIX/NFS file systems, NetWare DOS/MS Windows users are subject to sophisticated NetWare security. This is beyond what is currently available in the NFS protocol architecture for the UNIX users. UNIX/NFS files and directories mounted by the NFS Gateway benefit from NetWare security (Trustee Rights and file/directory attributes) as well as the usual UNIX permissions.

To visualize this, imagine two security doors. Each NetWare user request has to pass through both doors before it is granted access to the file or directory. When a NetWare user makes a request for file/directory access, the NFS Gateway checks to see if the user has the appropriate NetWare rights. If so, it converts the NetWare request into an NFS request and sends it to the remote NFS server where the file resides.

Figure 8: Method 2 enforces tight security.



The NFS requests contain the UID and GID(s) of the requestor, which are obtained from the NetWare-to-NFS mapping for users and groups. The NFS server then scrutinizes the NetWare user's request for NFS file access using its own UNIX/NFS security semantics. These include read, write and Execute/Search privileges for a file's owner, group owner or "others." The NFS server then performs the requested operation or rejects it. User's requests fail if either of the two security doors are closed because of insufficient security permissions.

Enhanced Security. In NetWare, access permissions can be set for a specific user in a group without removing that user from the group. For example, a group of users need to be given "All" rights to all files in a directory except for one file. NetWare allows you to make this file accessible to one user and invisible to everyone else. You do so by making the group "Everyone" the trustee of the file and granting it no rights, then making the specific user a "User" trustee of the file and granting the appropriate rights. The Novell NFS Gateway supports full NetWare security semantics for UNIX/NFS volumes.

NFS Server Work Offloaded by Gateway Caching. The NFS Gateway caches data at the server during NFS read and write operations according how you configure the NFS volume. When you turn on the read-ahead option for a volume, the NFS Gateway reads more data from the remote NFS server ahead of time than what is requested. This makes the data readily available at the NFS Gateway when the client requests it, rather than waiting for the request to return to the remote NFS server.

When you turn off the write-through parameter for a configured volume, the NFS Gateway does not "flush" data written to the NFS server right away, but caches NetWare client data at the Gateway server and flushes it later. Thus the Gateway handles a certain amount of I/O and processes some of the requests without having to send the requests to the remote NFS server. Every NFS request from an NFS client does not necessarily translate to an NFS request by the Gateway to the NFS server.

The NCP packets between the NetWare workstation and the NFS Gateway are 1KB in size, compared to 8KB UDP packets between the NFS server and the Gateway. This means improved response time for users on Gateway volumes configured with read-ahead and deferred write to the NFS server.

Simplified Gateway Management. The NetWare NFS Gateway can be administered from any TCP/IP system that supports the X Window System (UNIX) or VT100/220 terminal emulation (PC). The Gateway can also be administered from another NetWare NFS Gateway server console by logging in through NFSCON, the NFS Gateway administration utility.

Server-Based Authentication. NFS security relies on authentication being performed by the NFS client systems. This would be the NetWare 3 server where you install the NFS Gateway software. The NetWare server authenticates DOS and MS Windows users as they log in. The users have to quote valid usernames and passwords before accessing NetWare resources and thus prior to accessing Gateway volumes.

Unlike a typical (PC)NFS client, there is no need for a separate authentication daemon running in one of the NFS servers on the internet. Moreover, if a user has Supervisor privileges on a particular NetWare server, he or she can only change 1) the NetWare user information in the bindery, and 2) the NetWare-to-NFS user mapping in the NIS maps of that server only, but not on other NFS Gateway servers.

Disadvantages of the Server-Based Method

Disadvantages are as follows:

Server RAM Requirements. Figure 9 shows the memory used by essential Netware Loadable Modules (NLMs) that make up the NetWare NFS Gateway software. These modules use approximately 1.5MB of server memory. The cache buffers used by the Gateway software take up additional memory as well.

Figure 9: Memory required by NetWare NFS Gateway NLMs.

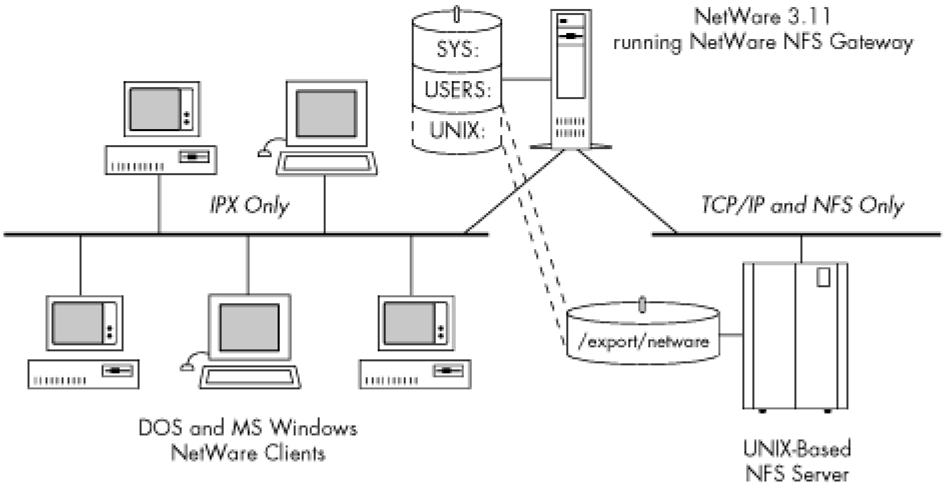
NetWare Loadable Module	Module Size (KB)	Size in RAM (KB)
NFSGW	1100	1100
LOCKD	131	121
STATD	21	16
NAMED	46	39
NETDB	70	58
NISBIND	27	21
NISSERV	32	25
PKERNEL	122	105
DISPATCH	23	18
XCONSOLE	80	71
Total	1652	1574

The NFS Gateway shares server memory with other NLMs installed on the same server. You can use a dedicated server to avert performance "hits" or downtime if several users are accessing NFS file systems through the Gateway, or if the Gateway needs to mount large sprawling file systems.

Server Loading. The NFS Gateway can become a bottleneck to network throughput as more NetWare users access the remote NFS file systems residing in various servers. The added workload affects Gateway performance because there is a finite number of processes and cache buffers that can cater to NCP requests from several NetWare workstations.

Greater Bandwidth Utilization. The NFS Gateway can also affect network bandwidth utilization. For a single NFS file read operation, the data may go on the same wire twice (NFS server to NFS Gateway; NFS Gateway to workstation). This happens if the requested data is not found in the NetWare NFS Gateway server cache. It is more than likely that the requested data will be in the NFS Gateway server itself, since the Gateway performs data caching during data reads and writes (if read-ahead is turned on and write-through is turned off).

Figure 10: Bandwidth problem alleviated using two LAN adapters in the NFS Gateway Server.



One way to alleviate this problem is to add another LAN card for the Gateway server, as shown above. One card can be connected to the main Ethernet backbone and another to the IPX network, separating the IPX and IP networks. With this configuration, NetWare IPX/NCP traffic will not impact the bandwidth on the Ethernet backbone network that has NFS and TCP/IP traffic.

Single Point of Failure. When you stop the NetWare NFS Gateway, all clients of the Gateway server that have drives mapped to gateway volumes will lose their connections. Other NetWare users can stay logged in. The remote NFS servers might be still running. NetWare users who are accessing the NFS file systems through this gateway must wait for the NFS Gateway to be restarted. But the users can access the NFS file systems through another NFS Gateway if that Gateway is configured to mount the same NFS file systems.

However, mounting the same NFS file systems from two different Gateways in the same workgroup can produce inconsistencies in the shadow file information for the Gateway volumes. The shadow files contain NetWare Directory information for each file accessed on remote NFS file systems. One shadow file is created for each configured Gateway volume when it is first mounted at the Gateway server. The shadow file expands as more files and directories are accessed on the remote file system. Depending on how the Gateway volumes are configured for trustee rights and other configurable options, users can get different views of the same remote file system if they access it through different Gateways. If the NetWare server goes down, users cannot access NetWare resources or any remote NFS systems through this particular Gateway.

Summary

Using NFS client software on PCs or using the NetWare NFS Gateway at the NetWare 3 server are two viable approaches for providing PC users with transparent access to remote NFS file systems. The NetWare NFS Gateway approach is a server-based NFS client solution for existing NetWare networks. The NFS Client for LAN WorkPlace is a good NFS client solution which can be used either with or without NetWare.

The (PC)NFS solution is ideal for the following:

- Committed TCP/IP users who need access to UNIX files.
- Organizations with business-critical data stored on UNIX systems but who need to offer PC users access via TCP/IP.
- Existing LANs with TCP/IP products already installed in all the PCs that provide TCP services like Telnet and FTP.

The NetWare NFS Gateway is targeted at these kinds of users:

- Users in a NetWare environment who may not be TCP/IP experts but need to access data on NFS servers.
- The NetWare user community at a university or other institution that needs casual access to UNIX data.
- NetWare environments that have NetWare 3 servers available to act as NFS Gateway servers.

Appendix A: Comparison of Novell's Solutions

	NetWare NFS Gateway 1.1	NFS Client for LAN WorkPlace 2.3
Technology	**NetWare server-based NFS client solution. NetWare users that are logged into the Gateway can access remote file systems on various NFS servers through the NFS Gateway.**	Works peer-to-peer between the (PC)NFS client and the remote NFS servers.
Hardware/Software Requirement	**NetWare 3 server with 8MB RAM. ODI-supported network adapter for the NetWare NFS Gateway server.**	IBM PC XT/AT, PS/2 with 640KB RAM. MS-DOS v3.3 (or later). Novell DOS 5.0 (or later),and LAN WorkPlace for DOS 4.0 (or later). ODI-supported network adapter for the PC.
Ease of Software Installation	**Installation/upgrade of the software is done at the NetWare server. You don't need software at either the remote NFS server or NetWare workstations accessing the remote NFS file systems.**	Need to physically travel to each networked desktop and install the NFS client software. The source code for (PC)NFS user authentication daemon is compiled and installed either on one UNIX system on the internetwork or on each of the remote NFS/UNIX systems.
PC User Authentication	**NetWare server based.**	(PC)NFS Authentication server based. DOS has no notion of users as individuals. Authentication server gives UID and GID to users quoting valid usernames from their PCs. Password checking is done when a DOS drive is linked to a remote NFS system.
Protocol Stack	**Concurrent access to Netware and NFS resources using a single protocol stack (IPX/SPX).**	Uses two stacks on the client for concurrent access to NetWare and NFS (TCP/IP for NFS connection and IPX/SPX for NetWare connection).
Configuration	**Done centrally at the Netware NFS Gateway server which needs only one IP address.**	Each workstation must be configured separately with an unique IP address.

Configuration of NFS Mounts	**Gateway volumes are configured and mounted at the NetWare NFS Gateway server. NetWare users that are logged into the Gateway have access to all the mounted gateway volumes. Access depends on user's trustee rights on the NetWare side and NFS permissions on the UNIX side.**	Each PC user must link drives to remote file systems on the NFS servers. They can customize the drives to suit their needs. The access to file and directories in the remote NFS file system solely depends on the UNIX permissions of Read, Write, Create/Search privileges for a file/directory owner, group owner or others.
Name Services Support	**DNS/NIS client and server support.**	DNS client support.
Administration Interface	**Server-based administration at the NetWare server console.**	DOS and Windows-based administration at the PC.
DOS/NetWare Commands and Utilities Support	**DOS and NetWare commands and utilities are supported for all the Gateway volumes.**	Only DOS commands are supported. Even if the workstation has IPX/SPX loaded, NetWare commands and utilities cannot be used for linked drives.
UNIX Commands Support At the PC for Linked Drives	**chmod, chown, chgrp, ls**	chmod, chgrp, ls
Seamless Integration of PC LANs-to-UNIX	**Remote NFS file systems appear as NetWare volumes to a NetWare user. No change to workstation software necessary.**	Remote NFS file systems appear as DOS drives to the PC user. PC users need to link drives to remote NFS systems.
Printing Support	**Not supported. Need to use products like FLeX/IP or NetWare NFS, which provide PC-UNIX print integration.**	DOS printer ports can be redirected to print queues that are defined in /etc/printcap files of remote NFS/UNIX systems.
NFS File/Directory Name Mapping	**Users get a consistent view of the filenames through the Gateway, since the NetWare directory information for the files accessed are stored in a "shadow file" for each Gateway volume.** **This is particularly meaningful with long UNIX filenames. If an NFS file "longfilename1" is referred to by the DOS filename "longfil0," it will stay the same even after you dismount and mount the Gateway volume. This is true as long as the corresponding Gateway volumes**	Every time a PC user links a drive, the user will get a view of the filenames in the file system, which depends on current changes on the NFS side, since the filenames themselves are not stored anywhere on the PC. The software does UNIX-to-DOS filename mapping each time the PC user links a drive to NFS file system. For example, if there are two files on the NFS side called "longfilename" and "longfilename1" with the first 8 characters being the same, the PC

	remains configured. Another new file on the NFS side called "longfilename2," will get mapped to "longfil1" on the DOS side, and so on.	user will see the corresponding DOS filename which depends on which file is being accessed and is based on the what the mapping algorithm comes up with.
File System Security	**NetWare trustee rights, NetWare file and directory attributes, and NFS file and directory permissions.**	NFS file and directory permissions only.
Autonomy	**NetWare Supervisor controls the NFS environment for the NetWare users. The users may have some privileges depending upon the rights assigned to them by the Supervisor to configure Gateway volumes or modify user or host information etc.**	The user has total control over his/her PC environment. He/she can change the configuration of linked drives, LAN board, IP address etc.
NFS Traffic	**Less NFS traffic if servers are spread throughout the net on different subnets. All NFS traffic channelled through the Gateway.**	NFS traffic from each PC goes directly across routers to the remote NFS servers.
Workstation Memory and Resources	**Eases client memory requirements. Workstation use no memory or resource to send an NFS request.**	The LWPNFS software takes up RAM when loaded on the PC. The PC sends NFS requests to the remote NFS system without going through an intermediary system or gateway.
Networked Environment	**Suited for NetWare users in a NetWare environment when NetWare 3 servers are available to act as NFS Gateways.**	This solution is suited for TCP/IP networks with LAN WorkPlace for DOS 4.0 or later installed on the PCs. No NetWare is needed.