Data General

Data General Corporation, Westboro, Massachusetts 01580

Customer Documentation

NetWare® for AViiON® Systems: Concepts

069–000483–01

AViiON®
PRODUCT LINE

NetWare® for AViiON® Systems: Concepts

069–000483–01

For the latest enhancements, cautions, documentation changes, and other information on this product, please see the Release Notice (085–series) and / or Update Notice (078–series) supplied with the software.

Printed in the United States of America
Rev. 00, October 1992

Ordering No. 069–000483

Notice

NetWare® for AViiON® Systems: Concepts
069–000483–01

Revision History:
Original Release – May 1990
First Revision – October 1992

Effective with:

DG/UX 5.4.1 or 5.4.2
NetWare® 3.11 for AViiON® Systems, Rev. 2.00

This manual includes extensive changes from the previous revision; therefore, we have not used change bars.

Certain portions of this document were prepared by Data General Corporation and the remaining portions were prepared by Novell Corporation.

Contents

How to Use This Manual

The *Concepts* manual is designed as an extended glossary of terms related to the NetWare® for AViiON® Systems product.

The concept entries are arranged alphabetically, with each alphabetical section beginning a new page.

If a concept is not explained completely in one part of *Concepts*, you are referred to a "See" or a "See also" reference where that concept is explained in detail. For example, the entry **Account, user** refers you to **User**. Go to **User** for the complete explanation of a user account.

Some entries refer you to related utilities in other manuals. For example, the entry **Shareable attribute** contains an explanation and then refers you to FILER, FLAG, and NDIR in the *Utilities* manual. Refer to the *Utilities* manual for more information about these utilities.

This manual uses abbreviated titles (shown in italics) when referring to other manuals in the NetWare for AViiON Systems document set, as follows:

Abbreviated title	Full title or Description
Administration	*NetWare® for AViiON® Systems: System Administration*
DOS Client	DOS workstation documentation
Installation	*NetWare® for AViiON® Systems: Installation*
Macintosh® Client	Macintosh workstation documentation
Messages	*NetWare® for AViiON® Systems: Troubleshooting and System Messages*
OS/2® Client	OS/2 workstation documentation
Print Server	*NetWare® for AViiON® Systems:* Print Server
Utilities	*NetWare® for AViiON® Systems: Utilities*

AAA

Access Control right

A NetWare right that allows users to modify trustee assignments and Inherited Rights Masks. At the directory level, this right allows users to modify both directory and file trustee assignments and Inherited Rights Masks. Users can grant any right (except Supervisory) to any other user, including rights that they themselves have not been granted. Since the DG/UX™ operating system allows disk space restrictions to be assigned, users can modify them using the Access Control right.

If more than one user is assigned to the directory, the Access Control right allows a user to modify the restrictions.

At the file level, this right allows users to modify only the file's trustee assignments and Inherited Rights Mask. Users who have this right can grant any right (except Supervisory) to any other user, including rights that they themselves have not been granted.

Use the letter **A** to represent this right.

See also **Inherited Rights Mask; Rights; Security; Trustee rights.**

Access privileges

Any of the following rights that control access to files or directories:

- **Read.** Open and read files. If granted in a directory, you can read all files in the directory (except for files that have had the Read right revoked). If granted in a file, you can read the file even if you do not have the Read right in that file's directory.
- **Create.** Create a directory (has no effect when granted for files).
- **Write.** Open and write to the file.
- **Erase.** Delete a directory or file.

- Modify. Change the attributes of a directory or file. Rename the file or directory.

- File Scan. See the filename when viewing the directory. See the directory structure from the file to the root of the directory.

- Access Control. Modify file trustee assignments and Inherited Rights Mask. Users who have this right can grant all rights, except Supervisory, to other users. They can grant the Supervisory right only if they are supervisors themselves.

- Supervisory. Grant all rights and enable any user who has this right to grant all rights to any users and groups for the file or directory in which the user has the Supervisory right.

See also **Inherited Rights Mask; Rights; Security; Trustee rights.**

Account, user

See **User account.**

Accounting

An option in SYSCON that allows network supervisors to charge users for file server use. The network supervisor can

- Install accounting on a file server;

- Select methods of charging for file server resource use;

- Select the service to be charged for;

- Determine the amount charged for each service;

- Monitor file server use.

Accounting Options

Once the network supervisor has installed the accounting feature, NetWare for AViiON Systems tracks user logins and logouts automatically and stores the information in the NET$ACCT.DAT file in the SYS:SYSTEM directory. (The file server does not charge for tracking logins and logouts.) Accounting also provides the following options—the supervisor can choose the ones that are suitable to the specific network environment.

- **Charging each user's account for resources consumed.** These charges can be made by the file server or by other types of servers such as print servers, database servers, or gateways. The network supervisor can decide which servers have the right to charge users.

- **Tracking and charging users for more than one service.** The network supervisor decides which services to charge for. If a particular accounting option is not necessary for that environment, the supervisor should not use that option.

- **Charging users for the disk space they use.** To use this option, the network supervisor must specify the amount that should be charged for disk storage. The supervisor also must specify how often and at what times the file server should measure the disk space users are using and charge their accounts.

- **Charging users for the time they use.** Users can be charged for the time they are logged in.

- **Charging users for file server requests (such as read or write requests) they make.** The file server measures the number of requests made by

    1. The amount of data the user requests the file server to read from its disks;

    2. The amount of data the user requests the file server to write to its disks;

    3. The number of requests the user makes of the file server.

The network supervisor can set up accounting to charge for some or all of these services. If the supervisor installs accounting but chooses not to charge for services, user logins and logouts are still tracked.

The supervisor can view system accounting records with PAUDIT.

Accounting Servers

When the network supervisor sets up accounting in SYSCON, he or she authorizes the current file server to charge for services. The supervisor can authorize other network servers to charge for the services they provide. The supervisor can also revoke a server's right to charge.

Charge Rates

The file server can charge for five types of services:

- **Blocks Read** allows the setting up of charge rates for the amount of data read from the server. The supervisor can specify the amount charged for each block read, in half-hour increments.

- **Blocks Written** allows the setting up of charge rates for the amount of data written to the disk. The supervisor can change the charge rate in half-hour increments.

- **Connect Time** allows the setting up of charge rates for the amount of time a user is logged in to a server. The supervisor can change the amount charged in half-hour increments. The charge is assigned per minute.

- **Service Requests** allows the setting up of charge rates in half-hour increments for service requests. A service request is any request made of the file server, such as listing the files in a directory. The charge is assigned per request reviewed.

If the network supervisor plans to charge users for services, he or she needs to calculate the amount to charge. The amount charged depends on the network environment.

Before setting charge rates for services, the supervisor should

- Determine what the services are and the amount that should be

charged over a given period of time.

- Determine what services to charge for and the amount to be made from each service. For example, if file server storage capacity is a concern, the supervisor should set the system up to charge for disk storage. If network use is high, consider charging for service requests. To discourage users from staying logged in when they are not working, the supervisor should charge for connect time.

- Estimate how much each service is being used by monitoring the file server for two or three weeks. For example, if 30% of the file server's charges stem from service requests, the supervisor could recoup 30% of the cost through charging for service requests.

At the end of the monitoring period, use ATOTAL to determine total use for each service. ATOTAL is run from the SYS:SYSTEM directory, so you must have Supervisor rights to that directory.

After having determined the amount to be charged for each service as well as how much each service was used, the supervisor can calculate the charge rates.

The charge rate is the charge per unit of the specified service. Charge rates are specified as multipliers and divisors. This multiplier/divisor ratio is used to change the amount of service usage to a monetary charge. The unit of charge is arbitrary, but begin with one charge unit equaling one cent. Adjust this ratio if it does not work for your network environment.

Use the formula below to calculate a charge rate for services.

$$\frac{\text{Charge (charge rate multiplier)}}{\text{Estimated usage (charge rate divisor)}} = \text{Total charge}$$

For example, if the network supervisor wants to charge $100 a month for blocks read services and he or she finds that 250,000 blocks were being read each month, then the charge rate would be 100 dollars divided by 250,000 blocks, or 4 cents per block read.

The supervisor needs to make the necessary conversion to cents (assuming one charge is equal to one cent) per block. See **SYSCON** (*Utilities*) for examples on how to assign charge rates for services.

Account Balances

The supervisor can

- Assign a user an account balance that determines how much of a given service the user can use.
- Assign a credit limit indicating how much credit the user can draw upon.
- Assign a system or default account balance. An account balance is assigned automatically to any user created after the default account is set up.
- Increase a user's account balance. The user must log out and log in again before any account balance changes are put into effect.

IMPORTANT 

If the supervisor installs the accounting option on a file server, he or she needs to carefully monitor account balances. The supervisor should warn users that if they are told to log out because their account balances are too low, they should log out immediately.

If users do not log out, the file server will automatically log them out. Users will lose any data that has not been saved.

Remove Accounting

To deactivate and completely remove the accounting feature from the file server, the supervisor must first delete all accounting servers. After having deleted the last accounting server, the supervisor can remove the accounting feature.

Related utilities: **ATOTAL; PAUDIT; SYSCON** (*Utilities*).

Account restrictions

See **Security**.

Active hub

Hardware that amplifies transmission signals in certain network topologies. You can use an active hub to add workstations to a network or to lengthen the cable distance between workstations and the file server.

See also **Passive hub**.

AFP

(AppleTalk® Filing Protocol) A file system from Apple Computer, Inc. that allows data to be shared in AppleTalk networks.

See also **NetWare file system**.

Application

Software that makes calls to the operating system and manipulates data files, allowing a user to perform a specific job (such as accounting or word processing). An application is a tool that makes performing a function easier.

Standalone application. An application run from the hard disk of a self-contained, independent computer system. Only one user can access it at a time.

Network application. An application run on networked computers and shared by a number of users. Lock-out and file protection features (such as flags and trustee rights) are needed for network security purposes. A network application can take advantage of network resources like printers. Advanced network applications (such as electronic mail) allow communication between users.

Host-based applications. NetWare for AViiON Systems provides a general-purpose Inter-Process Communication (IPC) facility to allow communication between processes residing on the AViiON system and NetWare clients. In addition, NetWare for AViiON Systems provides support for NetWare Remote Procedure Calls (RPC) that allow developers to quickly and easily build server-based applications on AViiON systems.

Archive

To back up data files.

See also **Back up; Backup.**

Archive Needed attribute

See **Attributes; Security (Attribute Security).**

Asynchronous transmission

See **Serial communication.**

Attach

To establish a connection between workstation and file server. The file server assigns each workstation a connection number and attaches each workstation to its LOGIN directory.

When a user logs in, the NetWare shell automatically attaches the workstation to the nearest file server.

Related utilities: **ATTACH; LOGIN; LOGOUT; MAP.**

Attributes

Properties of files and directories. Attributes override rights and prevent tasks that effective rights allow. They restrict or inhibit copying, deleting, renaming, viewing, writing, and sharing.

NetWare file and directory attributes do not match DG/UX operating system attributes, so NetWare for AViiON Systems stores attributes for each file ordirectory in an *NWinode* file in each volume. The information includes the attributes, creation time, and the creator of the file. See ***NWinode* file.** The following chart summarizes NetWare attributes and their functions.

Attributes	Letter	Directory	File	Description
Archive needed	**A**		✓	Identifies files modified after last backup. Assigned automatically.
Copy Inhibit	**C**		✓	Prevents Macintosh users from copying a file. Overrides Read and File Scan rights. Modify right required to remove this attribute.
Delete Inhibit	**D**	✓	✓	Prevents users from erasing directories or files. Overrides Erase right. Modify right required to remove this attribute.
Execute Only	**X**		✓	Prevents copying or backing up files. Attribute cannot be removed. Assign only to files with an .EXE or .COM extension (program files). Keep a duplicate copy of these files in case they become corrupted and need to be replaced. CAUTION: Some programs will not execute properly if flagged Execute Only.
Hidden	**H**	✓	✓	Hides directories and files from DOS DIR scans and prevents them from being deleted or copied. Directories and files appear in NetWare NDIR scans if a user has the File Scan right.
Indexed	**I**		✓	Not currently used by NetWare. Can be set, but has no effect.
Purge	**P**	✓	✓	Purges a file as soon as it is deleted if the file is flagged with this attribute or resides in a directory flagged with this attribute.
Read Audit	**Ra**		✓	Not currently used by NetWare. Can be set, but has no effect.
Read Only/ Read Write	**Ro/Rw**		✓	Indicates whether a file can be modified. All files are flagged Read Write when they are created and can be modified unless the Read Only attribute is set. Assigning Ro activates Delete Inhibit and Rename Inhibit. Modify right required to remove the Ro attribute.
Rename Inhibit	**R**	✓	✓	Prevents users from renaming directories or files. Modify right required to remove this attribute.
Shareable	**S**		✓	Allows several users to access a file simultaneously. Usually used in combination with the Read Only attribute.
System	**Sy**	✓	✓	Assign to system files and their directories. Hides these directories and files from DOS DIR scans and prevents them from being deleted or copied. Directories and files appear in NetWare NDIR scans if a user has the File Scan right.
Transactional	**T**		✓	Not currently used by NetWare. Can be set, but has no effect.
Write Audit	**Wa**		✓	Not currently used by NetWare. Can be set, but has no effect.

Related utilities: **FILER; NDIR; FLAG** (for files); **FLAGDIR** (for directories).

BBB

Back up (verb)

To copy a file, directory, or volume onto another storage device (such as a floppy diskette or a hard disk) so that the data can be retrieved if the original source is corrupted or destroyed.

Backup (noun)

A stored copy of a file, directory, or volume preserved as a safeguard in case the original is corrupted or destroyed. Backup in NetWare works with normal procedures currently in effect on DG/UX operating systems.

Base I/O address

The beginning address of an I/O port. The base I/O address allows the microprocessor to find the correct port for communicating with a particular device. See also **Base memory address; Interrupt.**

Base memory address

A configuration option found on some network interface boards. Network interface boards often use the base memory address as a buffer. When the network or device attached to the board sends information before the processor is ready, the information is placed in a buffer. Since the address for each device is unique, the memory address of each buffer should also be unique. A common source for hardware conflicts within a machine is to have two devices trying to use the same memory address for a buffer.

See also **Base I/O address; Configuration options; Interrupt.**

Baud rate

See **Printing; Serial communication.**

Bindery

A database that contains definitions for entities such as users, groups, and workgroups. The bindery allows the network supervisor to design an organized and secure operating environment based on the individual requirements of each of these entities. The bindery is comprised of three components: objects, properties, and property data sets.

Objects represent physical or logical entities, including users, user groups, workgroups, file servers, print servers, or any other entity that has been given a name.

Properties are the characteristics of each bindery object. Passwords, account restrictions, account balances, internetwork addresses, lists of authorized clients, and group members are all bindery properties.

Property data sets are the values assigned to an entity's bindery properties.

The NetWare bindery consists of three separate files located in the SYS:SYSTEM directory: NET$OBJ.SYS (for objects), NET$PROP.SYS (for properties), and NET$VAL.SYS (for property data sets).

Example

When user STEVE logs in, the LOGIN program looks in the NET$OBJ.SYS for the object name to determine if he is a valid user. If an object by the name of STEVE exists, the program then looks in the NET$PROP.SYS file for the properties associated with that object (in this case, to see if a password property for user STEVE exists).

Finally, if object STEVE has a password property (he is a user, not a workgroup), the program prompts him for his password and compares this value with the value in the NET$VAL.SYS file that is assigned to the password property. If the two values match, STEVE is logged in and allowed to use that network's resources according to the values of other properties (such as account restrictions and trustee assignments) that exist for user STEVE.

See also **Object; Property.**

BIOS

(Basic Input/Output System) A set of programs, usually in firmware, that enables each computer's central processing unit to communicate with printers, disks, keyboards, consoles, and other attached input and output devices.

Block

A unit of stored data. In NetWare for AViiON Systems, the default block size is 4KB, or 4,096 bytes, of data. For example, a 40MB hard disk contains roughly 10,000 blocks of data storage area.

BNETX.COM

The NetWare shell program that uses the burst-mode protocol. The shell works with IPX, SPX, and a LAN driver to convert a standalone computer into a network workstation. Loaded into RAM each time a workstation boots, BNETX begins network transmission each time a workstation requires service on the network. (Other NetWare shells are NETX.COM, EMSNETX.EXE, and XMSNETX.EXE.)

See also **EMSNETX.EXE; IPX; LAN driver; burst-mode protocol; NetWare shell; NETX.COM; SPX.COM; XMSNETX.EXE.**

Boot files (DOS workstation)

DOS executable programs that

- Start up the workstation operating system and its other drivers;
- Load the NetWare shell;
- Gain access to the network.

The workstation boot process

This section explains NetWare DOS boot file information, the configurable files, and what commands are used in them.

POST Routine. When a workstation is booted, the power-on self-

test (POST) routine built into the ROM-BIOS checks all peripherals: memory, monitor, keyboard, printer, and hardware installed in expansion slots.

Boot Record. ROM-BIOS determines which device to boot from by checking the boot record. The boot record is on either a floppy diskette or a local hard disk. ROM-BIOS then loads a short program from the boot record to determine the disk format and the location of system files and directories.

System Files. Using the information in the boot record, the ROM-BIOS loads the COMMAND.COM command processor and the system files (including two hidden files, IBMBIO.COM and IBMDOS.COM).

DOS Files. When IBMBIO.COM is loaded, it checks for a CONFIG.SYS file. CONFIG.SYS contains commands to

- Install device drivers;
- Modify the number of disk buffers allocated for local drives;
- Increase the maximum number of open files DOS allows concurrently on local drives;
- Specify the country for country-dependent information.

(If you do not create a CONFIG.SYS file, DOS assigns default values.)

When COMMAND.COM is loaded, it checks for an AUTOEXEC.BAT file and executes it. (AUTOEXEC.BAT contains programs, utilities, and DOS commands.)

Optional DOS Files. The AUTOEXEC.BAT file can also load NETBIOS.COM, INT2F.COM (for applications that require IBM's NetBIOS), and other files required by the hardware.

NetWare Boot Files. Up to this point, a workstation boots like a standalone computer. Workstation AUTOEXEC.BAT files also contain many of the following commands to log in to the network.

- **LSL.COM.** The link support layer file enables the workstation to

communicate over several protocols.

- **IPXODI.COM.** IPX (Internetwork Packet Exchange) the protocol stack file which manages communications among network stations.

- **NE2000.COM.** The LAN driver (such as NE2000.COM or NE2.COM) provides communication between the link support layer and the network board.

- **NETX.COM.** NetWare shell file for memory up to 640KB

- **EMSNETX.EXE.** NetWare Expanded Memory shell file

- **XMSNETX.EXE.** NetWare Extended Memory shell file

- **BNETX.COM.** NetWare shell file for burst-mode protocol that does not use extended memory.

The AUTOEXEC.BAT file can also contain commands to change the workstation's default drive to the first network drive, to load additional files required by the hardware, to change the workstation prompt, and to execute additional commands. Once the workstation files are loaded, the system checks for a SHELL.CFG or NET.CFG file to make further modifications to the NetWare environment.

Which files are required? Four files must be on the master workstation diskette and have commands included in AUTOEXEC.BAT:

- LSL.COM

- IPXODI.COM

- The shell file (such as NETX.COM)

- The LAN driver file (such as NE2000)

If you are using remote boot, you will need to add RPLODI.COM after LSL.COM in AUTOEXEC.BAT and before the LAN driver file.

If you are using IBM Token-Ring or IBM PCnet networks, you need additional files. See your IBM Token-Ring or IBM PCnet manual.

Create a SHELL.CFG file if

- There are non-IBM workstations on your network;
- There are non-network applications on your network that require you to set local printers to zero;
- There are local printers attached to workstations or if some features of print headers and footers need to be customized;
- Some options used by IPXODI.COM, the shell (such as NETX.COM), and NETBIOS.COM need to be customized.

See also the *Netware Workstation for DOS* manual.

NOTE 

Your workstation can hang if you press the <Shift> <PrintScreen> keys on your keyboard when none of your LPT ports are captured and no local printers are attached to your workstation. To prevent your workstation from hanging, include the following in your SHELL.CFG file on your workstation boot diskette.

LOCAL PRINTERS = 0

The workstation will try to find a local port and will eventually stall. Please be patient—the workstation has not hung.

NET.CFG like SHELL.CFG contains configuration information for the workstation and is an ASCII text file created with any DOS text editor. NET.CFG enables more versatility with ODI workstations and requires the latest version of the shell (such as NETX.COM).

A workstation may require NET.CFG along with SHELL.CFG. In most situations, you do not need NET.CFG because the established defaults are adequate.

Workstation boot file examples

This section gives examples of files you can create to boot your workstation and enhance its performance.

CONFIG.SYS. Consider booting your workstation with the following capabilities. The workstation can use <Ctrl><Break> to break out of a program. The workstation has 640KB and works with a database. Because databases require extra memory buffers, you need to increase the number of buffers from 15 to 20. The workstation also has an enhanced standard input and output device driver. Include the following lines in your CONFIG.SYS file.

```
break = on
buffers = 20
files = 20
device = ansi.sys
^Z
```

Your DOS documentation lists the default values of the configuration commands.

AUTOEXEC.BAT. The following four examples show files for different configurations.

Example 1

For a microchannel workstation using DOS. The file sets the mode for a color/graphics monitor at an 80-character display width (MODE CO80). The network board in the workstation is an NE2000. The workstation has 640KB of RAM. AUTOEXEC.BAT displays the login prompt for a user on the file server ENTERPRISE (LOGIN ENTERPRISE/).

```
MODE CO80
LSL
IPXODI
NE2000
NETX
F:
LOGIN ENTERPRISE/
^Z
```

Example 2

For an industry-standard architecture (ISA) workstation. This AUTOEXEC.BAT prevents DOS from writing commands to the screen (@ECHO OFF), clears the current screen (CLS), creates a prompt to show the current directory (PG), displays the contents of an ASCII file (type screen.asc), loads the workstation files without displaying driver contents on the screen (IPXODI > NUL), sets the default drive to network drive F (F:), and enters the LOGIN command for user JEAN on file server ELIOT (LOGIN ELIOT/JEAN). (For this batch file to execute, ANSI.SYS must already be loaded in CONFIG.SYS.)

```
@ECHO OFF
CLS
PROMPT $P$G
TYPE SCREEN.ASC
LSL
IPXODI > NUL
TRXNET
F:
LOGIN ELIOT/JEAN
^Z
```

Example 3

For an industry-standard architecture (ISA) workstation (XT or AT compatible). The file executes the initial workstation files (IPXODI and NETX), sets the drive to C (C:), and sets the prompt to show the current directory path (PROMPT PG). The user must change to a network drive before logging in.

```
LSL
IPXODI
NE2000
NETX
C:
PROMPT $P$G
^Z
```

Example 4

For a color/graphics monitor at an 80-character display width. The file is written for a workstation using a microchannel network board (3C505). The workstation has an attached mouse and needs to run a driver for it. The batch file sets the default drive to network drive F (F:).

```
MODE CO80
LSL
IPXODI
3C505
NETX
MOUSE1\MOUSE
F:
^Z
```

SHELL.CFG. The following file is written for a non-IBM workstation on a network using several versions of DOS. Therefore, the SHELL.CFG file needs to designate a long machine type for the login script to load the correct version of DOS (long machine type = compaq). The workstation uses a mail program (read only compatibility = 0), and it doesn't have local printers attached to it (local printers = 0).

```
long machine type=compaq
read only compatibility = 0
local printers = 0
^Z
```

Boot files (NetWare for AViiON Systems server)

Executable files and processes that start NetWare for AViiON Systems as a process on the DG/UX operating system and allow NetWare workstations to gain access to NetWare files on the AViiON system host.

Boot record

A file that contains information that ROM-BIOS uses to determine which device to boot from. The boot record can be on either a floppy diskette or a local hard disk. ROM-BIOS then loads a short program from the boot record to determine disk format and the location of system files and directories. Using this information,

ROM-BIOS loads the system files (including two hidden files, IBMBIO.COM and IBMDOS.COM) and the command processor (COMMAND.COM).

Bridge

A device that retransmits packets from one segment of the network to another segment.

A router, on the other hand, is a device that receives instructions for forwarding packets between different topologies and determines the most efficient path. See also **Router**.

Buffer

See **Cache buffer**.

Burst-mode protocol

A connection-oriented protocol built on top of IPX that controls message size and the rate of NCP read/write requests (and replies) larger than one packet. It enables a NetWare client to make a single request and receive a file in multiple packets. It also monitors duplicate, dropped, or out-of-order packets.

This protocol is more efficient than the one-request/one-response protocol in earlier NetWare versions. Formerly, the client would make a request for the first part of the file, receive the first 1KB packet, send a request for the next 1KB packet, receive the next 1KB packet, and so on until the file was downloaded from the file server.

With the new burst-mode protocol, network traffic is minimized. For example, a client sends only one read request for the file server to deliver a 250KB executable file. The file server sends back the requested file in several messages (containing packets of a pre-negotiated size). The client monitors the burst of incoming packets to make sure they are all received.

When a client writes a 1MB file to the file server, the client determines the number of write requests to send. It sends the first write request and the first part of the file (in packets of a pre-

negotiated size) to be written. The file server sends confirmation. Then the client sends a write request for the second part of the data and the next part of the data (in packets) to be written. This continues until the file server has received all data for the file. Then the file server writes the file as contiguous blocks to disk.

During this process, the client monitors packets to make sure they are all received and dynamically adjusts the size of the messages from 1KB to 64KB depending on the network board and the traffic on the wire. In heavy network traffic, when packets are dropped, the protocol dynamically slows the speed of the packets and reduces the message sizes to minimize lost packets. Under good network conditions, the protocol speeds up the packets and increases the message size for future replies.

NetWare for AViiON Systems is packet-burst aware on the host. To make the client packet-burst aware, load the VNETX.COM shell files on the client.

Bus

A signal route for transmitting data between various parts of the network. Several devices can be connected to a single bus, allowing them to share the same data pathway.

Data bus is the primary bus inside a personal computer.

Network bus is the main network cable or line that connects workstations.

CCC

Cabling system

See **Topology.**

Cache buffer

A block of file server memory (RAM) in which files are temporarily stored. The size of this cache is set in the NWConfig file with the token *cache_block_size;* it should be set to match the DG/UX file system's block size.

See also the *System Administration* manual.

Cache Memory

A section of reserved memory used to improve file server access time. NetWare uses the host cache as its main cache.

Beyond relying on the host cache, NetWare keeps local caches (spot caches). For example, a read-ahead cache in local memory predicts what the next block request will be in a sequential file. Database requests cannot be predicted by this cache.

Information on file locking and trustee rights is kept separately in shared memory, which can be accessed by all processes simultaneously.

Character length

See **Serial communication.**

Charge rates

See **Accounting.**

Clear text

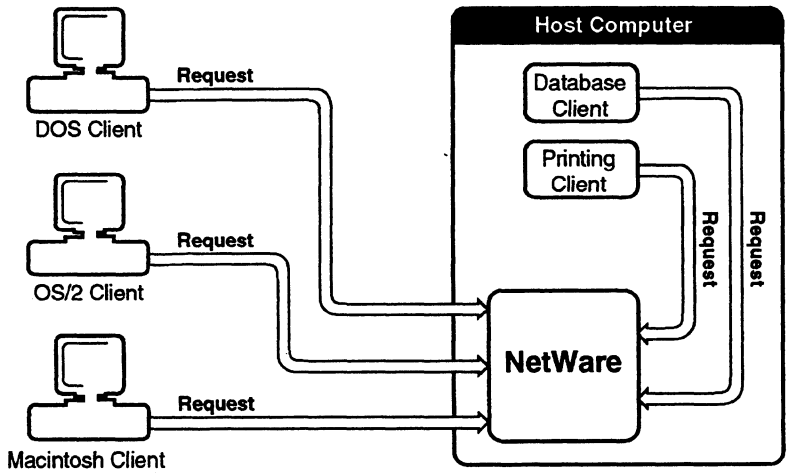
An unencrypted format for passwords. Used in versions of NetWare below v2.1, passwords are sent along the network in a clear text (unencrypted) format. However, this allows a protocol analyzer to read a login packet, which potentially could give an intruder access to a user's password. With NetWare v3.*x*, passwords are encrypted at the workstation in a format that only the file server can decode. This makes the network more secure.

See also **Encrypted Password; Security.**

Client

The software on a desktop computer that not only links it to a host computer running NetWare or an application that uses NetWare services, but allows the client to do part of the processing.

Clients initiate NetWare Core Protocol (NCP) requests to NetWare servers. The NetWare server initiates responses and does most of the storage and retrieval functions.



See also **DOS client, Host, Macintosh client, OS/2 client.**

CMOS RAM

(Complementary Metal Oxide Semiconductor Random Access Memory) Memory for storing system configuration data (such as number of drives, types of drives, and amount of memory). The CMOS RAM is battery maintained and is not available to the computer's operating system.

COM1, COM2

See **Serial port.**

Command format

A pattern that shows the proper way to enter a command at the computer keyboard. In NetWare manuals, a command format may include constants, variables, and symbols.

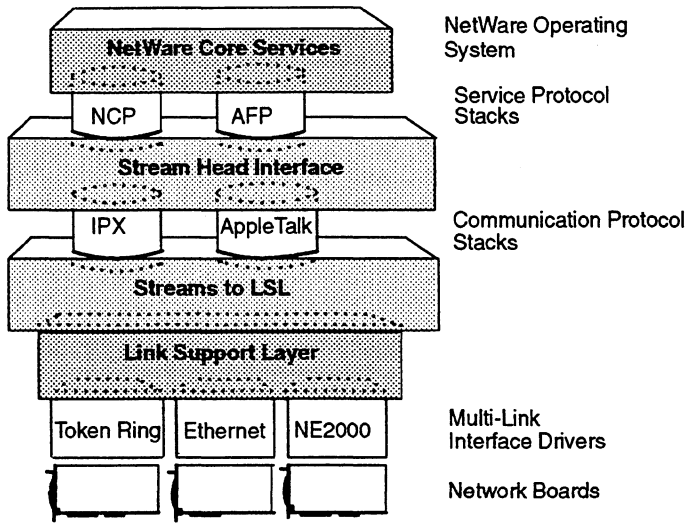
Communication protocols

A set of conventions or rules used by a program or operating system to establish communication between two or more endpoints. Many different types of communication protocols are used, although they all allow information to be packaged, sent from a source, and delivered to a destination system.

Workstation protocols. NetWare workstations use network board-specific protocols known as IPX (Internetwork Packet eXchange) and SPX (Sequenced Packet eXchange). Future versions of NetWare will use protocols such as NetBIOS, and AppleTalk (for Macintosh).

See also **IPX; SPX.**

File server protocols. NetWare for AViiON Systems has six layers of communication between an application and the AViiON system hardware. (See the following diagram.) In the AViiON system file server, the communication protocols allow the Service Protocol Layer to communicate with the Link Support Layer.



IPX, part of the operating system is the default communication protocol. As other protocols become available, you will be able to use more than one protocol on the same cabling scheme because the Link Support Layer allows a driver for a network board to service more than one protocol.

See also **Link Support Layer.**

Communications

See **Network communication; Serial communication.**

Configuration (hardware)

The equipment used on a network (such as file servers, workstations, printers, cables, network boards, and routers) and the way the equipment is connected: the physical layout of the network. Hardware configuration includes:

- The specific type of hardware installed in or attached to the computer, such as disk subsystems, network boards, memory boards, and printer boards;

- A specific set of parameters selected for a board.

Configuration options

Settings on network boards that allow all boards using the same cabling system to communicate with each other.

Configuration options can include four settings: interrupt, DMA, base memory address, and base I/O address. The way jumpers or switches are set determines the configuration number for a board. Most network boards are factory set to a default option (0). When more than one network board is installed in a workstation or file server, it means that the two boards will be using different cabling systems. Thus, the configuration options for those boards must be unique so that conflicts do not occur.

Interrupt

An interrupt setting on a board allows the network board to send an interrupt signal to the file server. The interrupt signal temporarily suspends the file server's operation. The file server can then perform the task requested by the interrupting device. Devices such as serial and parallel ports and network boards all need to have unique interrupts.

DMA

DMA (Direct Memory Access) allows some network boards and the workstation's memory to transfer information back and forth without having to go through the workstation's microprocessor. Typically, DMA channels 1 and 3 in a workstation are reserved for network boards. Other channels are dedicated to hard disk drives and floppy disk drives.

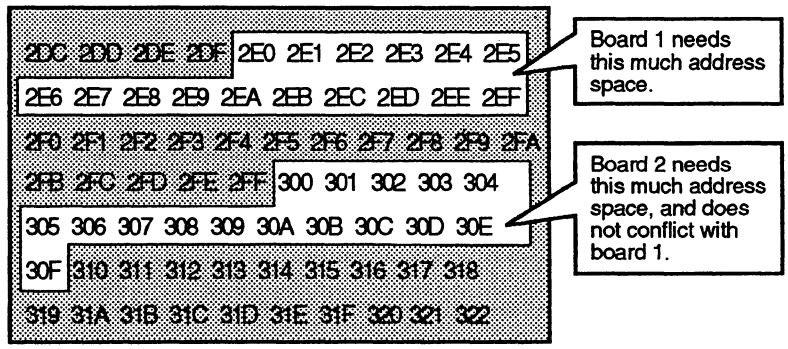
Base Memory and Base I/O Addresses

The base memory address and the base I/O address have separate physical locations in the computer. The base memory address is a range of memory used as a buffer. The base I/O address is the address of a port used to communicate with a device. The network boards are assigned a block of I/O or memory address space in the workstation where the network board and the operating system can transfer information to one another.

Preventing Setting Conflicts

The base address location for each configuration option is a hexadecimal number. (The file server operating system shows an extra 0 listed for the number. An address such as D0000 on the file server is the same as address D000 in the documentation.) The next hexadecimal number address for the next configuration option should be set far enough from the first number that the address space for one setting does not overlap the space reserved for the next configuration option setting.

Example



NetWare keeps track of used and free hardware settings. As you load disk drivers for the hardware devices in a file server, the system will not allow you to select a hardware option that conflicts with some other device in the system.

See also **Network number**.

Connection number

The number used by NetWare to control each workstation's communication with other stations. The number may be a different number each time a station attaches. To find your connection number, execute the WHOAMI or USERLIST.

Connection table

A table that tracks the following for workstations:

- Number of connections
- Peak connections used
- Connection time
- Network address
- Station address
- Number of requests made to the server
- Number of semaphore requests
- Number of records and files locked.
- Number of open files

View this information using *sconsole*, SLIST, and USERLIST.

Connectivity

The ability to link together different pieces of hardware and software (Macintoshes, PCs, minicomputers, and mainframes) in a network environment where resources (applications, processes, etc.) are shared. NetWare can also take advantage of existing host wide-area-network capabilities to interconnect remotely located NetWare LANs.

See also **Internetwork.**

Console, NetWare

A DG/UX terminal running *sconsole*, or a workstation that emulates a DG/UX terminal and runs *sconsole*.

See also ***sconsole***.

Copy Inhibit attribute

See **Attributes; Security (Attribute Security)**.

Create right

See **Rights; Security**.

Cylinders

Distinct, concentric storage areas on a hard disk (roughly corresponding to tracks on a floppy diskette). Generally, the more cylinders a hard disk has, the greater its storage capacity.

DDD

Daemon

A process running in the background that can spawn (initialize) other processes with little or no user input. Daemons provide services for clients, such as printing, remote printing, and server advertising. Some daemon processes such as the NetWare daemon perform administrative functions and access the host file system.

Data integrity

The accuracy, consistency, and completeness of data maintained by the host. The AViiON system provides the data integrity features of the NetWare for AViiON Systems product.

Data protection

A means of safeguarding data by maintaining duplicate file directories and redirecting data from bad blocks to reliable blocks on the hard disk.

The most serious failure in a network is generally a failure in the hard disks and their related hardware, since every user depends on continual access to the data stored on the file server's hard disks. Although a hard disk is a reliable and durable storage medium, areas of the hard disk's magnetic surface can, over time, lose the ability to store data reliably. If reliability is lost in the disk area where data is stored, data may be lost from files.

Protecting Data against Hard Disk Surface Defects

Host computer hard disks can store data in blocks of various sizes. These blocks are specific data storage locations on the disk's magnetic surface. Due to the constant reading and writing of data to the disk, some of these storage blocks can eventually lose their capacity to store data reliably.

If the host computer employs read-after-write verification, a block of data is written to a hard disk; then the data is immediately read back from the disk and compared to the original data that is still in memory. If the data from the disk matches the data in memory, the write operation is considered successful. The data in memory is released, and the next operation takes place.

Dedicated IPX drivers

The protocol stack workstation driver (IPXODI.COM) which manages communications amoung network stations. To link LAN drivers with other protocols, such as TCP/IP, load other ODI (Open Data-Link Interface) drivers. See the *NetWare for DOS* manuals.

See also **ODI.**

Dedicated mode

See **Routers.**

Default drive

The drive that a workstation is currently using. The drive prompt (such as A> or C>) identifies the default drive letter.

Default server

Usually the first server you log in to. The LOGIN command lets you change your default server.

Related utility: **LOGIN** (*Utilities*).

Delete Inhibit attribute

See **Attributes; Security (Attribute Security).**

Delimiter

A symbol or character that signals the beginning or end of a command or of a parameter within a command. For example, in the command CHKVOL A: B:, the blank space between A: and B: is a delimiter that marks two distinct parameters. Other delimiters include the comma (,), the period (.), the slash (/), the backslash (\), the hyphen (-), and the colon (:).

Device driver

See **LAN driver.**

Device sharing

The shared use of centrally located devices (such as printers, modems, and disk storage space) by a number of users. By attaching a device to a file server, which in turn serves several workstations, you can use resources more efficiently.

Directory

See **Directory structure.**

Directory attributes

See **Attributes; Security.**

Directory entry

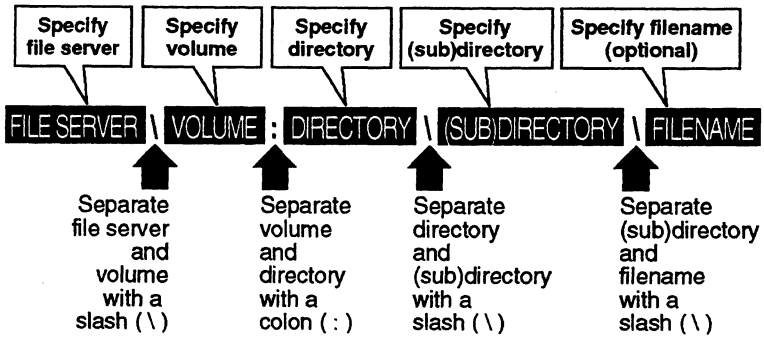
Basic file information, such as the

- Filename;
- File owner;
- Date and time of last update;
- First six trustee assignments;
- First block of the network hard disk in which the file is stored.

Directory entries are located in a directory table and contain basic information about the files on the volume. The file server uses the directory entries to keep track of the file's location, changes made to the file, and other properties related to the file.

Directory path

The name of the file server, the volume, and each directory leading down to the directory you need to access.



See also **Directory structure.**

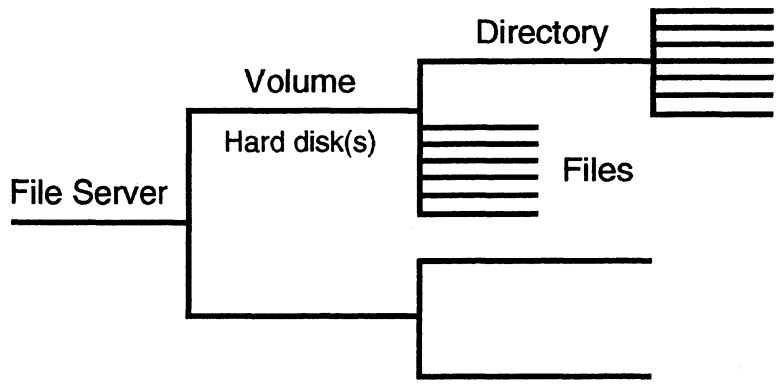
Directory rights

See **Rights; Security.**

Directory structure

The system used to organize network files on a file server's hard disk. Each file is given a filename and stored at a specific location in a hierarchical filing system so that files can be located quickly. The levels of this filing system begin with file server, divided into one or more

- Volumes, divided into
- Directories, which contain
- Files (and/or other subdirectories)

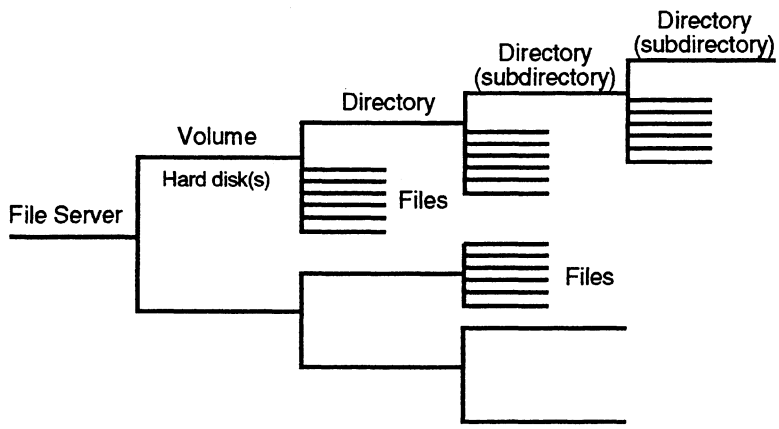


Volumes mark the start of the directory structure. (From the host AViiON system side, NetWare volumes appear as subdirectories within the DG/UX directory structure.) A volume is a logical unit; however, it behaves much like a hard disk to a standalone system. A volume may contain several physical disks. You can store directories at the volume level; storing files at this level is possible but, for security reasons, not recommended. See also **Host file system.**

Directories are places within a volume where you can store files or other directories. These directories-within-directories are sometimes called subdirectories. The term subdirectory is relative: a directory (A) is a subdirectory only in relation to the directory above it (B). When seen from a directory below it (C), the same directory (A) is a parent directory.

The hierarchically organized directories are commonly compared to an office filing system because the levels correspond to the filing cabinet, file drawer, hanging folders, and manila folders that contain the files.

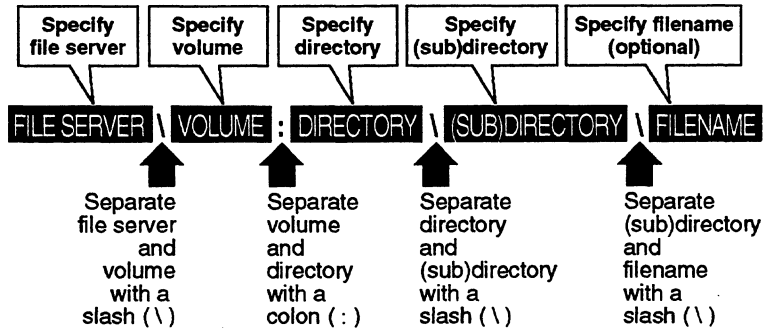
The analogy with an ideal filing system may be too neat, however. Just as some people place individual documents in the hanging folders or leave them loose in the drawers, files can be created in or copied to any level of the directory structure, from the directory level down. This means that a directory can contain any number of both files and subdirectories, as in the following tree structure.



Each directory is named when it is created. Because each level has a name, the location of any file can be pinpointed by listing the directory name at each level of the directory structure.

The list of levels constitutes both the directory path and the full name of the directory. Both begin optionally with the file server name and then specify volume, directory, and (if necessary) subdirectory and any levels below.

Use the following conventions when naming a directory or specifying a directory path.

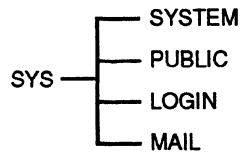


Replace *file server name, volume,* and *directory* with actual names in a specific directory structure. DOS files can have up to 8 characters; OS/2, or Macintosh files can have more. Although DOS recognizes only the backslash (\) for separating the levels of directory structure, NetWare recognizes either the slash (/) or backslash (\). The volume and the root directory (the directory next to the volume) must be separated by a colon (:). A directory path can optionally specify the filename.

As you plan directory structure for networks using more than one workstation operating environment, keep in mind the restrictions and parameters of the different systems if you intend to share files. For example, NetWare allows 255 characters (counting the drive letter and delimiters) in a directory path, but DOS permits only 127 characters. Some applications also restrict the path to the number of characters that will fit the screen width. Consult the documentation accompanying third-party applications to determine the maximum path length.

Basic Directory Structure

When volume SYS is mounted, it must contain the following four directories:



If these directories are not present, volume SYS cannot be mounted.

- SYS:SYSTEM is used for system administration and contains operating system files, NetWare utilities, and programs reserved for SUPERVISOR.

- SYS:PUBLIC is used for general access and contains NetWare utilities and programs for regular network users.

- SYS:LOGIN contains programs necessary for logging in.

- SYS:MAIL is used by NetWare-compatible mail programs. This directory also has an ID number subdirectory for each user that contains the user login script and print job configurations.

You create additional directories according to the needs of your organization. However, if your needs are better met by creating separate volumes, the volumes must be created when NetWare is installed. We suggest you create the following directories or volumes.

- One or more DOS directories. Create these directories in SYS:PUBLIC, since the appropriate security parameters (rights, attributes) are already set up. (See **DOS directories.**)

- One or more application directories. Create a separate directory for each application.

- A "home" or username directory for each user. If you want users to have personal workspace, create a separate directory (or volume) for this purpose.

You may also find the following kinds of directories useful.

- Work or project directories. If you want users to have group workspace or if you want to store completed application data files, create a directory for each project. You may want to create such directories in a separate volume to simplify backup.

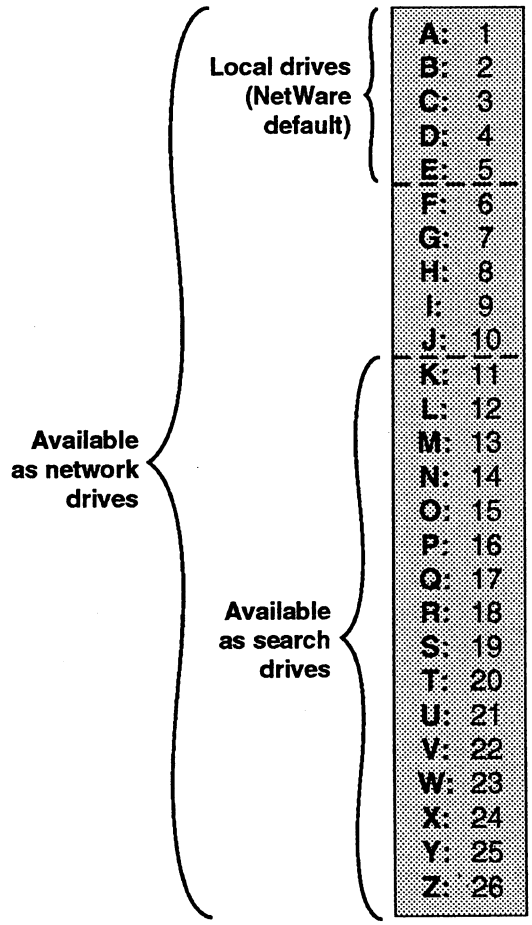
- A common directory in volume SYS (or a HOME or a WORK volume) to serve as an intermediate point in transferring files. (Assign group EVERYONE the rights necessary to copy files to and from this directory. If you do not want GUEST to have access to this directory, delete GUEST from group EVERYONE and assign GUEST only the rights you want temporary users to have.)

- A directory for storing batch files and utilities. If you do not want to store batch files in a public access directory, create a directory for your batch files elsewhere and assign rights to groups or individual users.

Accessing directories

Use DOS commands to access directories, but NetWare provides a more direct way by assigning drives to "point" to a particular location in the directory structure and by using search drives to execute program files that are in a directory other than your current directory.

The following figure shows the letters that can be assigned to either local, network or search drives.

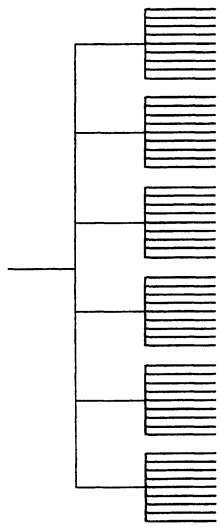


See **Drive mapping**.

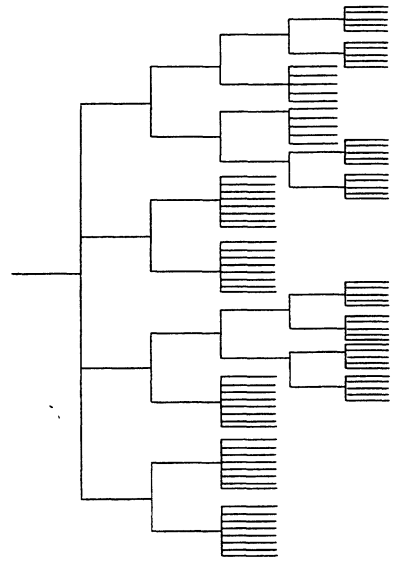
Types of Directory Structure

All directory structures are tree structures, but trees may have different proportions. Some are broad and spreading while others are tall and narrow. A directory structure may be relatively flat with many directories coming off the volume. Or your directory structure may be deep if you limit the number of directories at the root and create several levels of directory structure. The general principle is to keep directory structure clean and logical. Keeping the structure relatively flat (no more than five levels deep) generally increases its usability.

Flat Directory Structure



Deep Directory Structure



Plan directories by grouping your files logically. Plan subdirectory levels for natural subcategories.

Besides considering the logic of groupings, you may want to limit the number of files in each directory.

Determine which application allows the fewest characters in a directory path. You may need to plan either shorter directory names or a flatter directory structure.

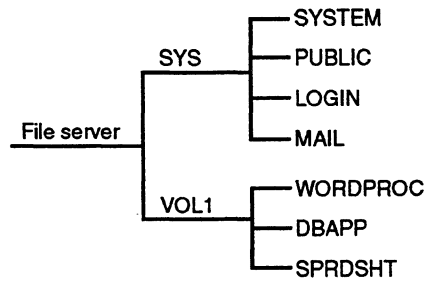
Types of Directories

You can create directories for both executabe files and data files. As network administrator, you must determine which types of directories best fit the needs of your network.

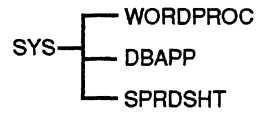
DOS Directories. Although DOS is the operating system used by individual workstations, it is installed on the network by copying DOS program files into network directories. You must create one or more DOS directories, copy the files into the directories, and then include a mapped search drive (usually Search2) in the system login script. (For more information, see **DOS directories.**)

Application Directories. Although applications can be accessed from local drives, installing them on the network provides the most convenient access. To determine the application directory structure that meets your requirements, first consult the documentation accompanying the software to see what is recommended or what possible adaptations you can make. Then plan a logical directory structure similar to one of the following.

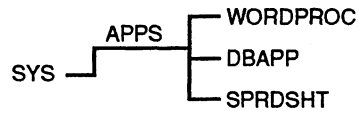
- A separate volume for applications with a separate directory for each application off the root. You must make trustee assignments for each application and map search drives in the system login script. This solution has the advantage of hiding applications from GUEST and of simplifying backup.



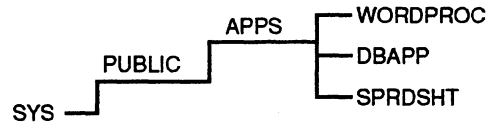
- A separate directory off volume SYS for each application. You must make trustee assignments for each application and map a search drives for each in the system login script. (However, some applications write files to the root. Since for security reasons you do not want users working at the root level, use MAP ROOT to map a drive to a fake root, in this case, a directory off SYS in which the user can be assigned rights.)



- A parent directory for applications, SYS:APPS, with subdirectories for each application. You must make trustee assignments for each application and map a search drive for each application in the system login script.



- A parent directory for applications, APPS, in SYS:PUBLIC. Because group EVERYONE has Read and File Scan rights in SYS:PUBLIC, you do not need to make trustee assignments or map a search drive. However, EVERYONE and GUEST can see and use all applications. Use this directory structure only if you want all users (particularly GUEST) to have access to all applications.



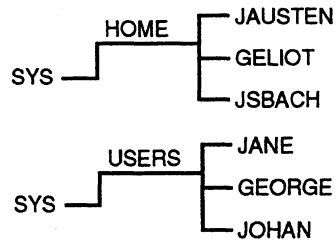
Do not install applications in the SYS:PUBLIC directory, unless a subdirectory is created for each application. Upgrading a network is made more complicated by mixing NetWare utilities with application program files. An application file might have the same filename as a NetWare utility file or another application's program file. In such a case, one file will overwrite the other because two files with the same filename cannot coexist in a directory.

Application data files can be created and stored in personal workspace in the home or username directory or in group workspace in separate work, project, or database record directories.

If the files are in each user's username directory, no other user (except SUPERVISOR or managers assigned file rights) can access them.

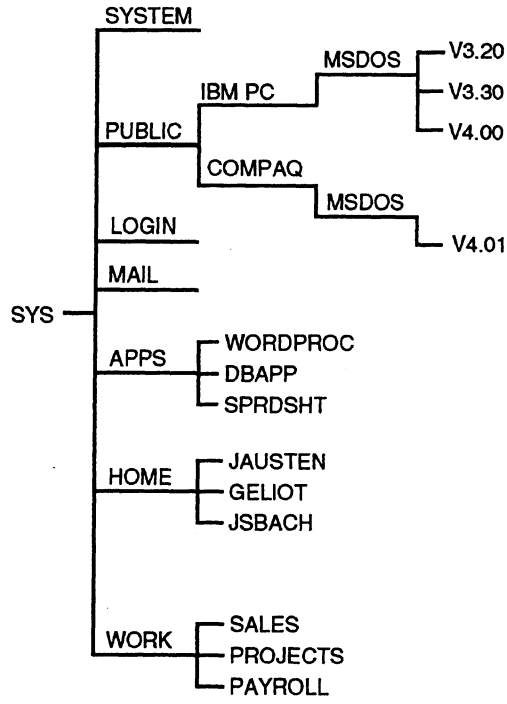
On the other hand, for your users to share data in group workspace, create work, project, or database record directories in SYS or another volume and then make trustee assignments for groups or users who need access to these directories.

Home or Username Directories. To provide personal workspace for users, create home or username directories. You can create a parent directory in the SYS volume called HOME or USERS. Then you can create a subdirectory for each user. The name of each subdirectory should be the username. Usernames can be up to 47 characters, but DOS will display only 8 characters in a one-level directory name. The username is usually composed of either the initials and surname or else the given name. See the following examples for both kinds of username directories.



Charting Directory Structure

To plan or keep track of directories, make a chart similar to the following. You do not need to create directories in SYS:SYSTEM, SYS:LOGIN, or SYS:MAIL (when you create each user, a subdirectory is automatically created to store the user login script and print job configurations).



See also **Attributes; Directory; DOS directories; Drive mapping; Rights; Security.**

Related DOS Utilities: **CD** (Change Directory); **DIR; MD** (Make Directory); **RD** (Remove Directory).

Related NetWare Utilities: **CHKDIR; CHKVOL; FILER; FLAGDIR; LISTDIR; MAP; NDIR; RENDIR; SYSCON** (*Utilities*).

Disable

To turn off; to render inactive. For example, the login token in the NWConfig file allows the system supervisor to disable all logins (except the login for SUPERVISOR).

Disk

A magnetically encoded storage medium in the form of a plate (also called a platter). Two types of disks are used with personal computers: hard and floppy. Hard disks use a metallic base and are usually installed within a computer or disk subsystem. (In some cases, this storage medium is removable.)

Floppy disks (called diskettes) use a polyester base and are always removable.

See also **Data protection; Enable; Hard disk; Partitions.**

Disk controller

A hardware device that controls how data is written to and retrieved from the disk. The disk controller sends signals to the disk drive's logic board to regulate the movement of the head as it reads data from or writes data to the disk.

Disk partitions

See **Partitions.**

Disk subsystem

An external unit that attaches to the file server and may contain hard disk drives, a tape drive, or both. The disk subsystem gives the file server more storage capacity.

DOS client

The software on a desktop computer that boots with DOS and gains access to the network through a NetWare shell or virtual terminal software. See also **Client.**

DOS directories

The location on the host where DOS files are stored. You can access DOS from local drives; however, it is more convenient to copy DOS program files and utilities to the network. To install DOS on the network, create one or more network directories for DOS and then copy the DOS files to the DOS directory.

To give users access to DOS directories, make a trustee directory assignment with the Read and File scan rights [RF] to group EVERYONE. If you include a mapped search drive (usually Search2) in the system login script, all users whose workstations require DOS can execute DOS commands from any location in the directory structure.

To plan for DOS directories, first determine

- DOS version
- Workstation brand (IBM brand is default)

Your planning is simplified if you have only one brand of workstation, or if you run only one version of DOS.

IBM Personal Computers and Same DOS Version

Even if all workstations on your network are IBM computers using the same version of DOS, you still need a separate DOS directory for the DOS program files. We do not recommend copying DOS files to SYS:PUBLIC. The DOS files would be mixed with NetWare utilities in a directory that contains many files. In such a case, upgrading is difficult.

Create a subdirectory in SYS:PUBLIC and name it for the DOS version, using the V*x.xx* naming convention as in the following example.

```
SYS:PUBLIC/V3.30
```

Load the DOS program files in that directory and map a search drive similar to the following in your system login script.

```
MAP INS S2:=SYS:PUBLIC\V3.30
```

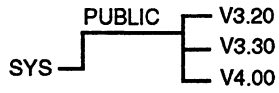
IBM Personal Computers and Multiple DOS Versions

To run more than one version of DOS, create a separate DOS directory for each version. Separate directories prevent the files from being overwritten, and also make it possible for each workstation's NetWare shell to direct workstation requests to the appropriate DOS directory. The shell contains information that can be read by the login script interpreter, and the login script sets the DOS environment that directs the searches for the appropriate DOS directory.

To use three versions of DOS, create directories similar to the following.

SYS:PUBLIC/V3.20
SYS:PUBLIC/V3.30
SYS:PUBLIC/V4.00

The directory structure would be similar to the following.



Although you have a different directory for each version of DOS, map only one search drive for DOS in the login script. Since the directory name follows the convention V*x.xx*, use an identifier variable for the directory named for the DOS version:

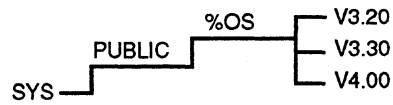
```
MAP INS S2:=SYS:PUBLIC\%OS_VERSION
```

IBM-Compatible Workstations

If your network has all IBM-compatible workstations, you can still use one of the solutions discussed for one or more DOS directories, as long as you use the format V*x.xx* for the directory name.

One Workstation Brand and Multiple DOS Versions

If all workstations on your network are one brand and you plan to run more than one version of DOS, consider the following directory structure.



Note that the literal directory name %OS is identical to a generic identifier variable.

Again, the NetWare shell for each workstation will direct workstation requests to the appropriate DOS directory. When you use identifier variables, you need only one mapped search drive for DOS in the login script:

```
MAP INS S2: = SYS:PUBLIC\%OS\%OS_VERSION
```

Multiple Workstation Brands

If you have both IBM (the default) and non-IBM workstations, you have additional considerations. If your non-IBM workstations are IBM-compatible workstations and can run the same type of DOS (for example, running IBM PCDOS on COMPAQ workstations), you can treat them as though they were IBM workstations.

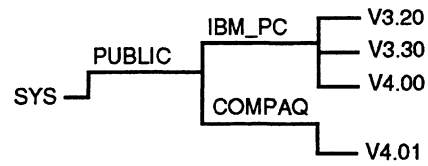
If you have both IBM and non-IBM workstations and your non-IBM workstations require a proprietary version of DOS (for example, COMPAQ DOS for COMPAQ workstations or Samsung DOS for Samsung workstations), you have additional tasks:

- Create a separate DOS directory for the proprietary DOS version.
- Assign the level of directory structure below PUBLIC a six-letter name that specifies the machine name (workstation brand). For example, you would use IBM_PC and COMPAQ. (If your workstation brand names have more than six letters, leave off the additional letters. For example, Samsung would be SAMSUN and Blue Chip could be either BLUECH or BLUE_C.)
- Set the LONG MACHINE TYPE command in the SHELL.CFG file on the boot diskette (discussed below) so the workstation's NetWare shell knows that non-IBM workstation brands run a proprietary version of DOS.

The directories should be named according to the following convention.

```
SYS:PUBLIC/machine name/DOS version
```

For example, suppose you have a network with both IBM and COMPAQ workstations. The IBM workstations run three versions of DOS, and the COMPAQs will run one version of COMPAQ DOS. In such a case, you would create four DOS directories, and we recommend that you create a directory structure similar to the following.



When you follow the naming conventions, you need only one search drive mapping for DOS in the system login script. You can use a generic drive mapping that provides access to specific DOS directories.

The following drive mapping corresponds to the previous example of DOS directory structure for multiple workstation brands.

```
MAP INS S2:=SYS:PUBLIC\%MACHINE\%OS_VERSION
```

To use the %MACHINE variable in the login script to indicate other than the default machine type (IBM_PC), set the following command in the SHELL.CFG file on each workstation's boot diskette (do not leave any spaces not indicated in this command format),

```
LONG MACHINE TYPE=name
```

Replace *name* with the six-letter name that specifies the workstation brand. In this case, replace *name* with COMPAQ.

NOTE

Even if you have only one DOS directory, you can use identifier variables in your system login script when you map a DOS directory to search drives. When you add another DOS version, you do not need to change the login script. Follow the same naming conventions.

USERDEF DOS Directories

To create users with the USERDEF utility, you can also let USERDEF create your DOS directories if you boot DOS and run USERDEF from one workstation that represents each unique combination of DOS version and workstation brand. (If you have six unique DOS version/workstation brand combinations, run USERDEF from one workstation of each combination.)In this case, the first time (and only the first time) you run USERDEF from each workstation, it will create a DOS directory for you and then prompt you to load DOS.

When USERDEF is run, the first instruction is to read the machine type and the DOS version as defined in the workstation's NetWare shell, see if a corresponding DOS directory exists on the file server and, if not, create a directory and path according to the strings found in the shell.

USERDEF then prompts you to insert the appropriate DOS diskettes, from which it copies the DOS files into the automatically created DOS directories.

USERDEF also provides a user login script that includes a search drive mapping to DOS directories:

```
MAP INS S2:=SYS:PUBLIC/%MACHINE/%OS/%OS_VERSION
```

This mapping contains an additional level of directory structure (indicated by the %OS variable) which corresponds to the directory path USERDEF creates. You will not be able to access DOS files if you modify the mapping, unless you have used the %OS identifier found in the NetWare shell.

See also **Directory structure; Login script.**

Related utilities: **FILER; USERDEF** (*Utilities*).

DOS ODI shell

(DOS Open Data-Link Interface shell) An interceptor for DOS services that determines whether requests from applications should be sent to DOS or to NetWare. The difference between the DOS shell and the DOS ODI shell is that ODI supports multiple protocols and multiple network boards in a single workstation.

ODI creates a "logical network board" to allow multiple frame formats over one network board and wire.

ODI offers the following benefits:

- You can expand your network by using multiple protocols (such as IPX/SPX, AppleTalk, or TCP/IP) without adding network boards to the workstation.
- You can communicate with a variety of workstations, file servers, and mini and mainframe computers through different protocol stacks without rebooting your workstation.
- You can protect your network board investment, because all protocols written to ODI specification can communicate through any network board written to ODI specification.
- You can spend less time and money on support. With one LAN driver supporting multiple protocols, you have fewer hardware components to support.
- You can use the NET.CFG file to configure the LAN driver for any possible hardware configuration.

Convert a standalone computer into a DOS ODI network workstation by adding one or more network boards, cable, the DOS ODI workstation software, and protocol suite software.

Three sets of files allow workstations to "talk" to each other, to the file server, and to other hosts.

LSL.COM

The Link Support Layer file enables the workstation to communicate using several protocols.

LAN drivers

Driver files such as NE2000.COM and TOKEN.COM communicate directly with the LAN boards. Drivers are also called MLIDs (Multiple Link Interface Drivers).

Protocol stacks

Files such as IPXODI.COM and TCPIP.EXE manage communications among network stations.

You may need additional files specific to the network product you are using.

See **NetWare DOS shell.**

DOS setup routine

The program that sets up the system configuration of your workstation or file server. It records the system's built-in features (boards, hard drives, disk drives, ports, math-coprocesser) and the available system memory. It also lets you choose date and time, password, and keyboard speed. The system configuration is accessed from the reference disk (for IBM PS/2® systems) or from the user diagnostics diskette (for most other systems). Instructions for running the DOS setup routine are usually contained in the introduction to your system's operations guide.

DOS version

The version of DOS (PCDOS, MSDOS, HPDOS, or CompaqDOS) for a personal computer. Different machine types (such as HP, IBM, or Corona) use versions of DOS that are generally not compatible. You need to inform the NetWare shell about the DOS version and the workstation type used, since it builds itself around DOS. Based on the information embedded in the shell, the shell descriptors (long machine name, short machine name, MSDOS, and DOS version) are read by the login script.

Since all DOS versions have identically named utilities and command interpreters, you cannot place the files of different DOS versions in the same directory. You must create a DOS directory for each workstation type/DOS version you use on your network and load the DOS files into it.

See also **Directory structure; DOS directories.**

Drive

A storage device, either logical or physical.

A physical drive is a storage device that data is written to and read from, such as a disk drive or tape drive. A drive that is physically attached to a workstation is called a local drive.

A logical drive is an identification for a specific directory located on a disk drive. For example, network drives read data from a specified directory on the network rather than from a local disk.

Drive mapping

A method of providing access to a specific location in the directory structure. NetWare recognizes two types of drives (physical drives and logical drives) and three types of drive mappings (local drives, network drives, and search drives).

Local Drives

Local drives point to disk drives installed in or attached to workstations. These drives may be floppy diskette drives or hard disk drives.

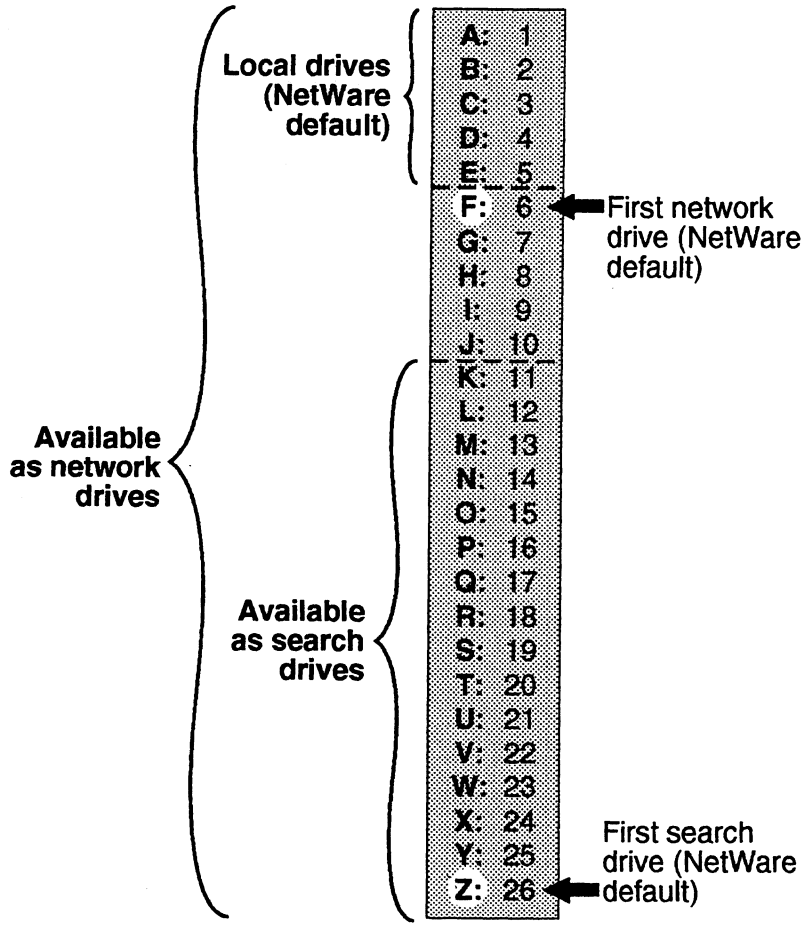
NetWare's default reserves a certain number of drive letters (A, B, C, and so on) for any local drives on a workstation. The first network drive is usually F. (To change the number of drive letters reserved for local drives, see your DOS manual for an explanation of the DOS LASTDRIVE command used in the DOS CONFIG.SYS file.)

See also **Directory structure; DOS directories.**

Network drives

A network drive serves the same function as a bookmark; it allows a user direct access to a particular location. To map a network drive to a directory, use the MAP command to assign a drive letter to represent the logical drive; then specify a particular directory path that leads to the desired point in the directory structure.

NetWare uses the letters of the alphabet to represent various data storage locations, or drives.



NetWare's default is for the first five letters of the alphabet (A through E) to point to local workstation drives. As SUPERVISOR, specify the drive letters for the drive mappings in the system login script.

Users who work at the command line or who want to modify their login scripts can assign the unallocated drive letters.
Users can map drive letters to different directories. One user may have drive J mapped to SYS:PROJECT\PLANS, while another user may have drive J mapped to SYS:HOME\JEFF.

With mapped drives, changing from one directory to another is quick and convenient. Rather than having to specify the entire directory path again, enter the drive letter followed by a colon.

When you use the MAP command at the command line, the drive remains mapped until you log out. To enter permanent drive mappings (at least until you change them), include them in a login script.

See **Login script**.

Search Drives

A search drive allows you to execute program files that are in a directory other than your current directory.

By mapping a search drive to a directory, you can access files in that directory even if you are working in another directory. When you request a file and the system cannot find it in your current directory, the system looks in every directory a search drive is mapped to.

To access DOS program files or an application from other directories, the system continues searching, following the numerical order of the search drives, until either the program file is found or cannot be located. (The SMODE command also searches for data files.)

Search drives are numbered (although they also have drive letters), and you should assign frequently used application or DOS directories to search drives in numerical order, beginning with Search1. Usually the first search drive (Search1 or S1) is also network drive Z; the second search drive (S2) would be network drive Y, and so on in reverse alphabetical order.

You can have up to 16 search drives out of the 26-drive total for each workstation.

Viewing Drive Mappings

When you log in for the first time (before system and user login scripts are created), a list of default drive mappings similar to the following appears.

```
Good morning, SUPERVISOR.

Drive A:    maps to a local disk.
Drive B:    maps to a local disk.
Drive C:    maps to a local disk.
Drive D:    maps to a local disk.
Drive E:    maps to a local disk.
Drive F:= AVIION\SYS:     \SYSTEM
 -----
SEARCH1: =Z:.[AVIION\SYS:     \PUBLIC]
SEARCH2: =Y:.[AVIION\SYS:     \]

F:>
```

In this example from the file server AVIION, drives A through E are mapped to local disks. This is also NetWare's default mapping. The first one or two local drive mappings usually correspond to floppy diskette drives.

Drives F, Y, and Z are network drive mappings. Drive F is the first network drive (NetWare default), and for SUPERVISOR, it is mapped to AVIION/ SYS:SYSTEM.

Drive Z is a search drive mapped to the SYS:PUBLIC directory. This search drive mapping allows you to access the NetWare utilities in the SYS:PUBLIC directory from any point in the directory structure. (Drive Y and drive Z are both mapped to SYS:PUBLIC. When you install DOS on the network, the DOS directory structure will be added to the path for drive Y.)

The last line of the screen display, "F:>" or "F>:\SYSTEM", indicates the default directory, the directory to which you are currently mapped. (The prompt is displayed as "F>\SYSTEM" only if you first set it to "PG" at the command line, in the AUTOEXEC.BAT file, or in a login script.)

Display your current drive mappings at any time by entering "MAP" at the prompt.

Use the MAP command in login scripts to establish a set of mappings that appear each time a user logs in.

Related utility: **MAP** (*Utilities*).

Driver

See **LAN driver.**

Dynamic memory

The most common form of memory, used for RAM. Dynamic memory requires a continual rewriting of stored information to preserve data. A continuous electrical current is necessary to maintain dynamic memory. All data is lost when the power supply is turned off. The speed of access to dynamic memory depends upon the RAM chip rating; usually between 60 and 150 nanoseconds.

EEE

Effective rights

The rights that a user can exercise in a given directory or file.

Directory effective rights are determined by trustee assignments, if they exist. Otherwise the effective rights of the current directory are determined by the intersection of the effective rights of the parent directory and the current directory's Inherited Rights Mask. No effective rights exist in a volume's root directory until you assign trustee rights.

File effective rights are determined by trustee assignments to the file if they exist; otherwise, they are the same as the directory effective rights.

See also **Security (File effective rights)**.

Related utilities: **FILER**; **RIGHTS**; **WHOAMI** (*Utilities*).

Embedded SCSI

A hard disk with a SCSI (Small Computer System Interface) and a controller board built into the hard disk unit.

See also **SCSI**.

EMSNETX.EXE

The NetWare expanded memory shell program that works with IPX, SPX, and a LAN driver to convert a standalone computer into a network workstation. Loaded into RAM each time a workstation boots, EMSNETX begins network transmission each time a workstation requires service on the network.

See also **Boot files**; **BNETX.COM**; **Communication protocols**; **IPX**; **LAN driver**; **Message packet**; **NetWare Expanded Memory shell**; **NetWare extended memory shell**; **NETX.COM**; **SPX**; **XMSNET.EXE**.

Enable

1. To turn on, especially to restore a feature that has been disabled.

2. To place in a state that will allow certain interrupts to occur in a processing unit (such as a network board). Interrupts are usually enabled by setting a switch or a jumper.

See also **Disable.**

Encrypted password

A password that is scrambled before it is stored at the file server, to prevent an intruder from viewing or copying it. Some encryption schemes encrypt the password at the workstation before it is transmitted to the file server. This prevents password monitoring over transmission lines.

See also **Clear Text; Password.**

Engine

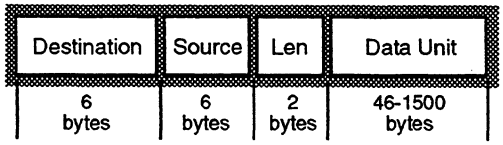
See **Process.**

Erase right

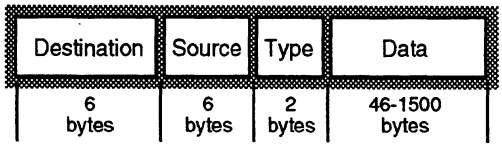
See **Rights; Security (Rights Security).**

Ethernet configuration

A configuration that allows network stations to communicate with each other by sending data in frames along an Ethernet cabling system. The IEEE 802.3 standard and the Ethernet II (or Ethernet) standard use different frame formats. Of the following illustrations, the first shows the IEEE 802.3 frame format, and the second shows the Ethernet II format.



IEEE 802.3 format



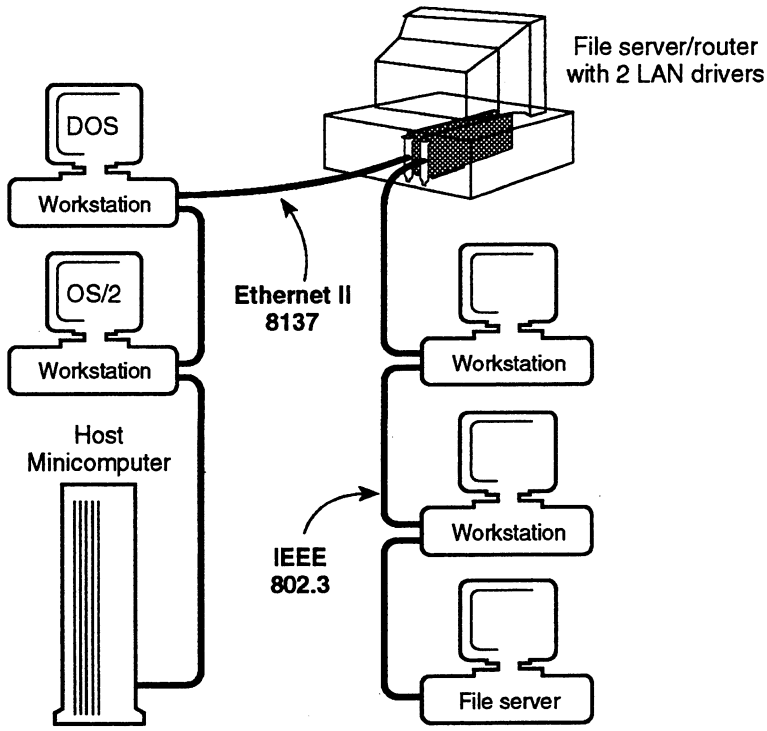
Ethernet II format

Ethernet II frames contain a unique protocol ID (represented in the "Type" field of the frame) that IEEE 802.3 frames do not contain. Network stations using the different standards cannot co-exist on the same Ethernet cabling system. However, Ethernet II stations using different protocol numbers on an Ethernet II cabling system can co-exist, but they cannot communicate with each other.

NetWare clients and routers use the IEEE 802.3 standard by default. However, you can configure file servers, workstations, and routers to use the Ethernet II standard. To do this, set the FRAME parameter in NET.CFG. (See "NET.CFG Options" in the *Installation* manual.)

Configuring workstations and routers. NET.CFG allows you to configure NetWare workstation shells and router software so that the Ethernet II standard can be used.

The following diagram illustrates how multiple networks can be configured on an Ethernet cabling system. NFAS supports both formats.



EVERYONE

A system-created group that includes all users created on the file server. Since group EVERYONE is already in the bindery as an object when the file server first comes up, users are added as members as they are created. Whenever all users need the same rights, you can grant those rights to group EVERYONE.

EVERYONE is automatically assigned Read and File Scan rights in the SYS:PUBLIC directory. These rights allow all users to run NetWare utilities, execute DOS commands, or access application programs residing in that directory.

EVERYONE is also assigned Create rights in SYS:MAIL. These rights allow any user to create and send mail to any other user; however, the user creating the mail cannot reopen the mail once it is sent to another user's mailbox.

The network supervisor can delete any user from group EVERYONE or change EVERYONE's trustee rights (including rights granted by the system) in any directory. However, we do not recommend removing EVERYONE's trustee assignments in the SYS:PUBLIC and SYS:MAIL directories. If users do not have trustee rights in the SYS:PUBLIC and SYS:MAIL directories, they cannot access NetWare utilities, use electronic mail, or use print job configurations unless you reassign these rights to each user.

Do not delete group EVERYONE. If group EVERYONE is deleted and then re-created, you must add all users to the group individually and reassign trustee assignments.

See also **Groups; User.**

Related utility: **SYSCON** (*Utilities*).

Execute Only attribute

See **Attributes; Security (Attribute Security).**

Expanded Memory shell

See **NetWare Expanded Memory shell.**

Extended attributes (EAs)

A high performance file system (HPFS) convention that allows information about a file to be attached to a file or directory. Operating systems such as OS/2 and NetWare store extended attributes from the file or directory so that the attributes do not affect the contents.

Each extended attribute has two parts:

- A name (null-terminated string)
- A value (text, bitmap, or binary data)

Standard extended attributes (SEA) conventions require that files begin with a period.

Some typical SEAs are .TYPE, .ICON, .HISTORY, .SUBJECT, .KEYPHRASES, .APPTYPE, and .ASSOCTABLE.

The application that creates the extended attributes and the applications that read the extended attributes must recognize the format and meaning of the data associated with the given name.

Extended Memory shell

See **NetWare Extended Memory shell.**

External router

See **Routers.**

FFF

Fake Root

A subdirectory that functions as a root directory. NetWare allows you to map a search drive to a fake root (a directory where rights can be assigned to users).

NOTE 

Fake roots work only with NetWare v3.0 and above with NETX.COM, BNETX.COM, EMSNETX.EXE, and XMSNETX.EXE. If you use older versions of the workstation shell, you cannot create fake roots.

Some applications cannot be run from subdirectories; they read files from and write files to the root directory. However, for security reasons, users should not be assigned rights at the root directory level. To use an application that must be installed at the root, you can load the files in a subdirectory and designate the subdirectory as a fake root directory, using a command in the login script similar to the following.

```
MAP INS ROOT S5:=SYS:APPS\NON_NET_APP
```

You cannot use the DOS CD (change directory) command at the fake root to return to the original root. To change the fake root back to the original root, you must remap the drive.

See also **Directory Structure; Security**.

Ferro-resonant isolation transformers

See **Power conditioning**.

File attributes

See **Attributes; Security**.

File caching

The method of holding recently-used data in cache memory to enable quick access to frequently requested files. NetWare for AViiON Systems uses read-ahead cache memory only. No general purpose cache is supported by NetWare because this would duplicate the caching performed by the AViiON system and possibly introduce errors in the cached data.

File compatibility

The ability to transfer file information transparently from the NetWare environment to that of the AViiON system and back again. Users wanting to copy files to and from the DG/UX environment may do so through terminal emulation, assuming access privileges are adequate. NetWare for AViiON Systems provides transparent file transfer, filename conventions, filename length, and filename extension support.

Files residing on the DG/UX host appear as DOS, OS/2, and Macintosh Finder files to the respective NetWare clients.

File extensions

The three characters that appear after the period in a DOS filename. File extensions can be:

- Assigned arbitrarily by an individual.
- .COM, .EXE, or .BAT to enable a file to execute a command, program, or batch file.
- .ERR or .DAT to indicate that the file has a unique function. For example, an .ERR file contains an error log file and a .DAT file contains an ASCII text file.
- Used to identify the file format (such as .ASC, .BIN, .GIF, .DFX, or .RFT).
- Assigned by certain companies.
- An indication that the file contains data associated with a specific programming language such as .C, .ASM, .BAS.

Some DOS and NetWare files share the same extension.

File extensions shared by DOS and NetWare	
EXE	DOS executable file
BAT	DOS executable batch file
DAT	ASCII text file
COM	DOS executable command file
ERR	Error log file
OVL	Overlay file used as part of NetWare files created from C-Worthy program to share code
HLP	Help screens which appear by pressing F1 in a menu utility
SYS	Operating system file

File locking

A means of preventing changes to a file. This ensures that a file is updated correctly before another user, application, or process can access the file.

For example, without file locking, if two users attempt to update the same word processing file simultaneously, one user could overwrite the file update of the other user.

See also **Record locking.**

File rights

See **Rights; Security.**

File Scan right

See **Rights; Security (Rights Security).**

File server

A host computer that runs the NetWare system software. NetWare for AViiON Systems enables a DG/UX host to store data for and regulate communications among the workstations attached to it and to manage any shared resources (such as printers). To function as a NetWare server, an AViiON Series system requires at least 16 megabytes of main memory, 200 megabytes of disk storage, and a QIC-150 tape drive.

Booting the File Server

The procedure for booting the file server is done by DG/UX.

Downing the File Server

The procedure for downing the file server is done by DG/UX.

Some maintenance procedures require that you down the file server. When you do this, the file server writes the data in memory to disk, thus preventing data from being lost. Users on the file server should be notified that the server is going down so that they can save and exit their files.

File server console operator

A user or a member of a group to whom SUPERVISOR delegates certain rights in managing the file server. A console operator has rights to use the *sconsole* utility. This utility allows the console operator to broadcast messages to users, change file servers, access connection information, view NetWare version information, change the system date and time, and enable or disable login for additional users.

See also **SUPERVISOR.**

Related utilities: ***sconsole;*** **SYSCON** (*Utilities*).

File sharing

A feature of networking that allows more than one user to access the same file at the same time.

See also **Attributes.**

File system

A collection of volumes, directories, files, and other structures that allow data to be stored and retrieved by name hierarchically. The file system also tracks the amount of space available on the medium.

Functionally, a file system is part of the operating system. The file system translates requests from an application program into requests that a disk driver can understand. Typical requests include instructions to manipulate a file (such as open, close, write, or create). NetWare for AViiON Systems performs file services by accessing the DG/UX file system.

File system interface

The ability of NetWare for AViiON Systems to allow the DG/UX operating system and NetWare to interact on files equally. NetWare files reside on a portion of the AViiON system's file system. NetWare handles the interface between NetWare files and the DG/UX file system. Only hybrid users can modify files, filenames, or directories with DG/UX editors. If other types of users modify files with host operating system editors, the users will cause unexpected, and often negative, effects.

See **Hybrid user**.

Flag

See **Attributes**.

Form

The name and size of the paper used for a print job in a NetWare printer command.

Frame

1. A variation of a protocol, such as Ethernet, Ethernet II, IEEE 802.3, or Token-Ring.

   See also **Ethernet configuration**.

2. A packet.

   See also **Message packet**.

GGG

Gateway

A link between two networks. It allows communication between dissimilar protocols (for example, NetWare and non-NetWare networks) using industry standard protocols such as TCP/IP, X.25, or SNA.

Generic file system (GFS)

See **NetWare file system.**

Groups

A way to simplify network administration by dealing with users collectively rather than individually. When users are created, they automatically become members of group EVERYONE and have the rights assigned to group EVERYONE.

You can create other groups based on who uses the same applications, printers, or print queues, who performs similar tasks, or who has similar needs for information.

Grant trustee assignments to directories and files through groups rather than users, which simplifies your job.

You can also use defined groups to simplify login scripts. By using groups (formed for common application use) and the conditional IF...THEN, you can map a search drive to that application directory. You can also use IF...THEN with a groupname to EXIT to a menu created for that group. Or you can prepare a login message to be displayed for group members when they log in. Use SYSCON and FILER to create groups and make group trustee assignments.

See also **EVERYONE; Login script; User.**

Related utility: **SYSCON; FILER** (*Utilities*).

GUEST

A username for anyone who needs temporary and restricted access to the file server. GUEST is present in the bindery as a bindery object when the file server is first brought up.

The network supervisor should evaluate the security needs of the network and determine whether to retain GUEST and, if retained, what rights temporary users can exercise and what information they can access. If someone needs to access the file server for a definite period of time, the supervisor might prefer to create a username and user account with an expiration date.

GUEST is automatically a member of group EVERYONE, and GUEST's rights come from membership in that group. As a member of group EVERYONE, GUEST is automatically granted rights in the SYS:PUBLIC directories. These rights allow users to run NetWare utilities, execute DOS commands, or access application programs residing in that directory.

GUEST is also assigned a mailbox and Create rights in the SYS:MAIL directory. These rights allow GUEST to create and send electronic mail, but not to reopen the mail once it has been sent to another user's mailbox. If the supervisor has made additional trustee assignments to group EVERYONE, GUEST has them as well.

The GUEST account has no initial password, but you can require one. Consider assigning GUEST a password and changing it frequently. Do not allow GUEST to change the password.

For maximum security, you can also take any of the following measures:

- Delete GUEST from group EVERYONE and make a specific trustee assignment to GUEST, such as EVERYONE's rights to SYS:PUBLIC, the DOS directory, and whichever application you permit GUEST to use.

- Delete GUEST from the file server if you have no temporary users.

If you want GUEST to have more privileges

- Assign GUEST temporary rights to specific directories and files;
- Create a GUEST subdirectory in the HOME or USERS directory to provide personal work space for GUEST.

See also **User.**

HHH

Handshaking

The initial exchange between two data communication systems prior to and during data transmission to ensure proper data transmission. A handshake method (such as XON/XOFF) is part of the complete transmission protocol.

A serial (asynchronous) transmission protocol might include the handshake method (XON/XOFF), baud rate, parity setting, number of data bits, and number of stop bits.

See also **Serial communication.**

Hard disk

A high-capacity magnetic storage device that allows a user to write, read, and erase data. Hard disks can be network disks or local workstation disks.

See also **Data protection; Partitions.**

Hardware interrupt

See **Interrupt.**

Hexadecimal

A base-16 numeric notation system frequently used to specify addresses in computer memory. In hexadecimal notation, the decimal numbers 0 through 15 are represented by the decimal digits 0 through 9 and the alphabetic "digits" A through F (A = decimal 10, B = decimal 11, and so forth).

Hidden attribute

See **Attributes; Security (Attribute Security).**

High performance file system (HPFS)

One of the features of OS/2 that supports hard disk partitions and files of up to 2GB in size, long filenames of up to 254 characters, and extended attributes (EA). Access is fast because the HPFS distributes file information across the hard disk rather than in a single table. In addition, the file and directory information loads into memory for quick access. Hard disk partitions can have a single disk volume of up to 2,000GB. HPFS also provides compatibility between OS/2 and DOS files. NetWare supports the HPFS.

See also **Extended attributes; File system.**

Home directory

A network directory that the network supervisor creates specifically for a user. The user's login script should contain a drive mapping to his or her home directory.

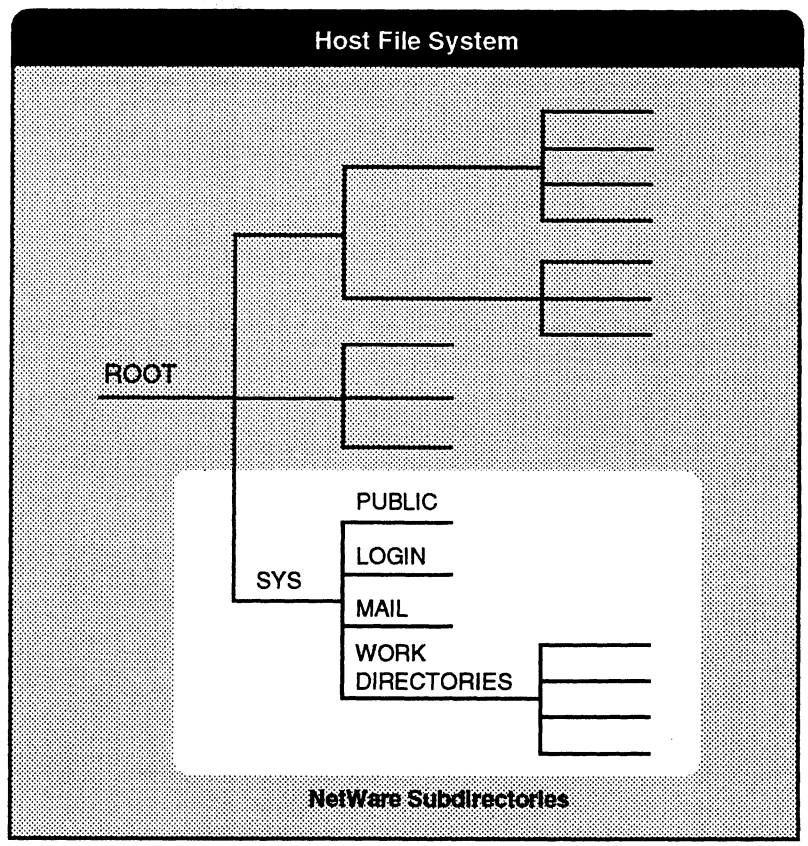
Host

The central computer or controlling computer in a timesharing or distributed processing environment, or the part of the host operating system that performs the storage/retrieval function. The host also detects bad data transfers and corrects them.

NetWare for AViiON Systems runs on an AViiON system as an application and emulates a NetWare file server by performing storage, retrieval, and management of data transfers as a process.

Host file system

The method that host computers use to stores files. File systems range from simple to complex depending on the operating system of the host computer. Most file systems are represented as tree diagrams with a single root directory and many subdirectories with files in the subdirectories. NetWare is installed in one of the subdirectories. NetWare for AViiON Systems uses the DG/UX file system as a resource in implementing the NetWare file system.

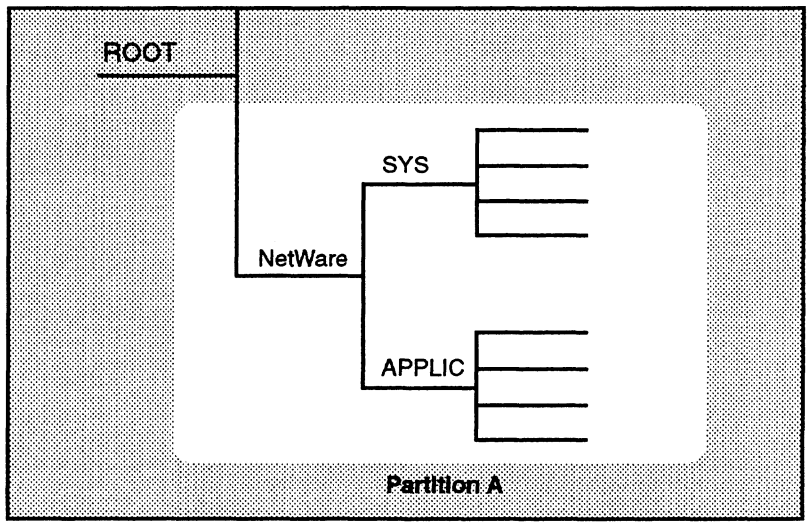


NetWare on the host file system

Some host file systems are one tree. However, parts of the tree can reside on separate devices or different logical partitions. Disks can be logically partitioned so that they appear as separate devices. Each logical partition has a file system. To the user, the multiple physical file systems appear as a single file system.

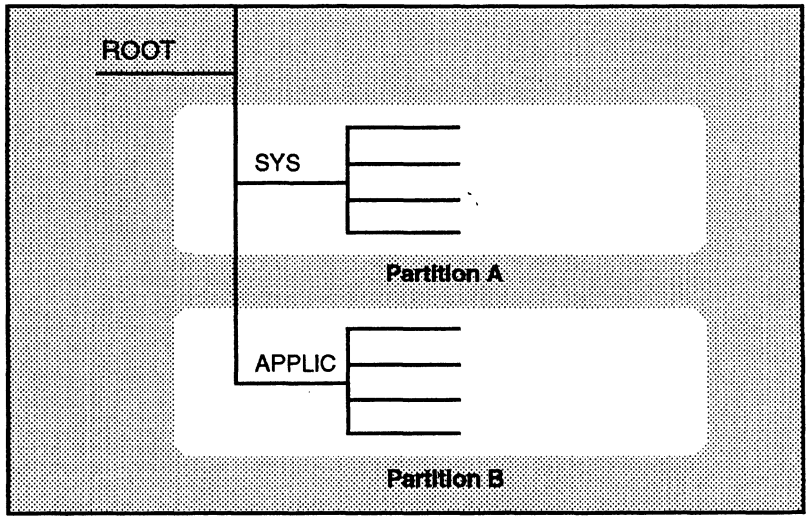
NetWare volumes are mount points in the DG/UX file system. If more than one volume is created on one partition of the file system, those volumes will show combined statistics (such as space available, total number of file objects, files in use, and files free).

To the NetWare user, the volume level appears to be the root; however, this is only one branch of the DG/UX directory structure.



NetWare volumes on the same partition

If volumes are created on different file systems (logical partitions), the volumes show separate statistics for each volume.



NetWare volumes on different partitions

Since NetWare works on top of the DG/UX file system, all NetWare file information is saved in the *NWinode* file, a volume-level file.

See also **Attributes; File system; Host file system; *NWinode* file; NetWare file system; Volume.**

Host operating system

A collection of system programs that own and manage resources on the host computer. The host operating system runs NetWare as a process in application space. NetWare for AViiON Systems, as a "sub-operating system," manages its resources through the DG/UX operating system.

The host operating system is responsible for

- Commands to the hardware devices
- Interface with the users
- Library routines for use by applications programs

UNIX®, VMS™, and AOS/VS are examples of other host operating systems.

Hub

A device that modifies transmission signals, allowing the network to be lengthened or expanded with additional workstations.

See also **Active hub; Passive hub.**

Hybrid user

A user who can own both NetWare and DG/UX files. The purpose of the hybrid user is to maintain rights across the two systems so that users can create files as NetWare users and still work with the files when logged in to the host and vice versa. When a hybrid user creates a file in a NetWare volume, whether as a DG/UX user or a NetWare user, the file is tagged with the host account ID.
A hybrid user holds a user account on the DG/UX system and one on NetWare. This user can log in to NetWare from a DOS, OS/2 or Macintosh client and manipulate files. The same user can also log in to the AViiON system and access those NetWare files through a host application, as long as the user has proper rights. NetWare attributes and file information are not available, however.

When a hybrid user logs in to NetWare, all of NetWare's security is enforced. This user can create, delete, and modify files only in NetWare volumes where rights are granted.

When a hybrid user logs in to the AViiON system, DG/UX security is enforced. Given rights by the host, the user can log in to DG/UX and delete, modify, and create files in the NetWare volumes even when the user does not have those rights granted under NetWare.

When a NetWare user with all rights logs in to the network, only the NetWare directory structure is visible. When a hybrid user with all rights logs in to the AViiON system, the complete DG/UX directory structure is visible, including NetWare volumes that the user has rights to.

The HYBRID utility allows the system administrator to connect a DG/UX-defined name (and user ID) to a NetWare user ID (a bindery object created with SYSCON). HYBRID assigns NetWare bindery properties to the DG/UX user ID and DG/UX group ID.

To access the host's directory structure, DOS hybrid users can use NVT to log in to the AViiON system. Files can then be copied from the DG/UX directory structure to NetWare volumes.

See also **NVT; HYBRID** in the *System Administration* manual.

III

Identifier

See **Login script**.

Indexed attribute

See **Attributes; Security (Attribute Security)**.

Inherited Rights Mask

The method of controlling which rights users can inherit. An Inherited Rights Mask (IRM) is given to each file or directory when it is created. The IRM for any given file or directory is modified by revoking rights. The directory's IRM controls which parent directory effective rights can be exercised in the current directory. The file's IRM controls which of the current directory's rights can be exercised in the file.

See also **Security (Rights Security)**.

Related utilities: **ALLOW; FILER** (*Utilities*).

Interleave factor

A method of adjusting the speed of the controller to match the speed of the hard disk. Typically, a hard disk spins faster than a controller can perform a read/write. If the controller is not fast enough to read or write consecutive sectors on a hard disk track, then the controller can be programmed to skip one or more sectors of the hard disk before the next read/write is performed.

If the controller reads or writes one sector and then skips a sector, the interleave factor is 2 (one out of every two sectors is used). The interleave factor is sometimes written as 2:1. If the controller reads or writes one sector and then skips two sectors (one out of every three sectors is used), the interleave factor is 3 or 3:1.

The interleave factor is usually established by the manufacturer or reseller of the hard disk/controller combination. If someone other than the manufacturer or reseller puts together the hard disk/controller combination, they may need to experiment to determine the correct interleave factor.

Internal router

See **Routers**.

Internal network number

See **IPX internal network number**.

Internetwork

Two or more networks connected by an internal or external router. Users on an internetwork can use the resources (such as files, printers, or disk drives) of all connected networks.

Interoperability

The ability of Native NetWare and NetWare for AViiON Systems to share a common architecture. NetWare for AViiON Systems provides integration of workgroup, departmental, and other NetWare networks, and acts as the link to the DG/UX environment.

Interprocess communication

The ability of two processes to communicate with each other or exchange data.

Shared memory, OS/2 named pipes, UNIX sockets, and NetWare streams are different mechanisms that enable existing programs to communicate with processes on other systems.

For example, in NetWare, the various processes communicate using variables stored in shared memory. Access to the shared memory is snychronized using a semaphoring mechanism.

Another example of interprocess communication is the use of a shared memory segment to hold the cells of a spreadsheet. Any process in the spreadsheet application (such as calculation, graphics, or printing) can act on any byte in the shared memory segment as needed.

Interrupt

A signal or call to a specific routine. The microprocessor suspends the current program until the routine is completed. The processor continues with the original program after the routine is completed.

Interrupts are divided into two general types: hardware and software.

A hardware interrupt is caused by a signal from a hardware device, such as a printer.

A software interrupt is created by instructions from a software program.

I/O address

See **Base I/O address.**

IPX

(Internetwork Packet eXchange) A Novell implementation of the XNS communication protocol that transports data (packets) between network devices (workstations, file servers, routers, etc.).

On a DOS client workstation, the shell (such as NETX.COM) determines whether to route requests to DOS or NetWare. The shell hands the data to IPX which puts an IPX header on it (specifying a source and destination network, node, and socket address). Next, the network board driver adds a media access control (MAC) header (including a source and destination node address) on the packet and sends it to the board and to the wire.

IPX packets transmit as datagrams (self-contained packages that move from source to destination). As IPX packets arrive at the correct sockets in the destination network station (for example, file services or print services) other protocols execute the service.

SPX, which monitors the transmissions to assure correct delivery, also uses the services of the IPX protocol for routing.

For clients, IPXODI.COM is a terminate-and-stay-resident file. To load other ODI drivers, see the *NetWare for DOS* manuals.

IPX on a NetWare for AViiON Systems server is a STREAMS driver which performs routing functions from within the DG/UX operating system.

See also **BNETX.COM; Communication protocols; LAN driver; Message packet; NetWare expanded memory shell; NetWare extended memory shell; NetWare DOS shell; NETX.COM; SPX.**

IPX internal network number

A logical network number that identifies the individual file server. The internal network number for each file server must be unique, hexadecimal, and from one to eight digits.

Related utility: **SCONSOLE** (*System Administration* manual).

See also **Network number.**

IRQ

See **Interrupt.**

Isolation transformer

See **Power conditioning.**

LLL

LAN driver

A set of software routines which understand and control the physical structure of a network board. A LAN driver serves as the connection between a network station's operating system and the physical network parts.

LAN drivers are specific to a particular network board. When you add the LAN driver to the NET.CFG file for a workstation, you allow the operating system to communicate on a network through the installed network board. IPX will pass information to the LAN driver and let the LAN driver direct the board on transmission procedures.

The file server also uses LAN drivers to communicate with network boards. The LAN drivers are linked below IPX in STREAMS.

See also **IPX; NetWare DOS shell.**

Line-surge suppressor

See **Power conditioning.**

Link Support Layer (LSL)

An implementation of the Open Data-Link Interface (ODI) specification. (The ODI specification is a network standard that specifies how multiple network communication protocols can operate on the same network.)

The LSL serves as an intermediary between the file server's LAN drivers and communication protocol, such as IPX, AFP, or TCP/IP. The LSL allows one network interface board to service several communication protocol stacks. The LSL also allows several network interface boards to service the same protocol stack.

See also **ODI.**

Local area network (LAN)

A network located in a building or a building complex. The maximum distance from one end of the network to the other, or from one node to another, is usually limited by the signal strength or the network's built-in time limit between sending and receiving messages. See also **Wide area network.**

Log in

A procedure that initializes the user's security rights and the user's environment by using the LOGIN command. When a user initiates a login request, the operating system scans the bindery and reads the user's bindery information into memory. The user is then asked for a password.

All security information is then placed into the file server's connection list and the user is said to be "logged in." At this point, the login program executes the login script to initialize environmental variables, map network drives, and control the user's program execution.

Log out

A procedure that breaks the filer server/workstation connection and deletes drives mapped to that server by using the LOGOUT command.

You can log out of one or more file servers at a time. For example, if you are connected to three file servers and you log out without specifying a file server name in the LOGOUT command, the workstation connections and mapped drives to all three file servers will be terminated.

If you want to log out of one file server and remain attached to the other servers, you must specify the file server name in the LOGOUT command.

Make sure that at least one of the remaining drives is mapped to the PUBLIC directory of a file server that you are still attached to. Otherwise, you will not be able to access any NetWare utilities. If you cannot access the NetWare utilities, you can use the DOS CD (Change Directory) command to find the PUBLIC directory. From there you can map new drives. It may be easier to log in to the file server again and allow your login script to set the drives.

The file server periodically checks each connection to see if it is still valid. The system manager can set a time limit on the file server's routine. If you do not log out before the specified time limit and your workstation has been inactive during the specified time, the file server will consider the connection invalid and will log out your workstation automatically.

Related utility: **LOGOUT**

LOGIN directory

A system-created directory (SYS:LOGIN) created during network installation; it cannot be deleted. The LOGIN and SLIST utilities are copied into the LOGIN directory. Users can log in and view a list of available network servers from this directory.

Login restrictions

The means to prevent a user from logging in. These apply to individual user accounts. When a user exceeds the login restrictions, NetWare disables the user account and no one can log in using that username. This makes it difficult for unauthorized users to log in. You can restrict login in the following ways.

Account Balance. If you have installed Accounting to regulate network resources, you can assign initial account limits for users. When the account is depleted, NetWare disables the account.

Expiration. You can specify an expiration date for a user account. The account expires at 12:01 a.m. the next day.

Password. You can require a password. You can also specify the minimum length of passwords, how often the password must be changed, whether the password must be unique, and whether the user can change the password. A unique password must be different from the previous ten passwords used by the account.

You can also specify the number of times a user can log in with an expired password or the number of incorrect login attempts. When that number is exceeded, the account is disabled.

You can view password restrictions by selecting a particular user in SYSCON.

If you allow users to change passwords, they can edit their own login scripts.

Connection Restrictions. You can limit the number of physical workstations from which a user can concurrently log in. You can also specify which physical workstations.

Time Restrictions. You can restrict the hours during which users can log in. You can assign all users the same hours, or you can restrict users individually.

Login script

A set of commands that initialize environmental variables, map network drives, and control the user's program execution. Login scripts are similar to configurable batch files and are executed as part of the login procedure.

After a user initiates a login request and supplies the correct username and password, the login program executes the login script.

System and User Login Scripts

NetWare uses two kinds of login scripts.

The system login script allows the network supervisor to set network drive mappings and search drive mappings for all users. It includes commands that should be executed for every user or for defined groups of users.

The system login script is created in SYSCON and saved in the SYS:PUBLIC directory (as NET$LOG.DAT). Because this file is stored in a general access directory, no passwords or proprietary information should be included in the system login script.

An individual user's login script, which executes after the system login script, specifies the user's individual drive mappings and environment variables.

A user login script is created for each user in SYSCON and saved as a LOGIN file in an ID subdirectory for that user in the SYS:MAIL directory.

You should create a system login script before you create user login scripts. If you access the box for a user login script in SYSCON and put in even a blank space, the system considers a user login script to exist and prevents the user from accessing the default login script when logging in.

For security purposes, each user should have a login script, however minimal. Since the login script is kept in the user's mail directory, it is possible for an intruder to create a login script file for any user who does not already have one. (The mail directory gives Create and Write privileges to other users to allow them to deliver electronic mail.)

A backup file, LOGIN.BAK, is created in each user's ID subdirectory when the login script is modified; this file can be renamed if you delete LOGIN by mistake.

Default Login Script

If no user login script exists, a default login script executes.

Consider using the default login script only temporarily. (If you continue to use the default login script and install DOS, you must create DOS directories that conform to the generic Search2 drive mapping. The directory level indicated by the identifier variable %OS should be named MSDOS. See **DOS directories** for more information.)

Login Script Conventions

When you create a login script, follow the command format described in Appendix A in the *Installation* manual. The command format specifies the proper syntax for keywords, variables, parameters, spacing, delimiters, or other characters and punctuation.

Login script commands are not case-sensitive; however, any identifier variables enclosed in quotation marks (such as those in the first line of the default login script, "%GREETING_TIME" and "%LOGIN_NAME") must be preceded by a percent sign (%) and typed in upper-case letters.

Only one command can be entered on each line, and command lines cannot exceed 150 characters. To increase readability, however, use only 78 characters per line—the width of your screen. Consider leaving a blank line between groups of commands; for example, put all mappings in a block set off from commands that come before and after.

When you type login script commands, be sure to press the Enter key at the end (and only at the end) of each command. If a long command continues beyond the width of the screen, the words that wrap onto the next line are still considered part of the command.

Use REMARK (and its aliases, asterisk (*), semicolon (;), and REM) to include explanatory comments so that you will have a record of the purpose of each command or block of commands. The comments and notes included in a login script with REMARK are not displayed when the login script is executed.

Commands Used in Login Scripts

Login scripts are interpreted a line at a time by LOGIN.EXE. The set of login script commands includes commands that have been assigned the same name as those of corresponding commands (with similar functions) in another system. Login script commands have been based on

- **NetWare utilities.** For example, the login script commands MAP and ATTACH have functions analogous to the NetWare utilities.

- **DOS commands.** For example, you can set DOS environment from within the login script because DOS BREAK, SET, and VERIFY have the same function in a login script.

Additionally, the login script command IF...THEN...ELSE is similar to conditional commands in most programming languages (and can also be nested in versions of NetWare above 3.0). The login script conditional allows both the use of identifier variables (such as date, time, login name, and station number) and command line parameters.

You can also use the login script to pass a command to the command line by including

- The pound sign (#) preceding the name of an executable file;

- EXIT (which terminates the login script) preceding the filenames of .COM, .EXE, and .BAT files. A filename must be enclosed in quotation marks. EXIT takes the information in quotes and puts it in the keyboard buffer as it terminates login.

The version of DOS you are running sometimes determines how you can use this function. For example, you can call up any internal or external DOS command by using #COMMAND /C only if you are running DOS 3.1 and above.

Commands such as WRITE and FDISPLAY, used only in login scripts, display text.

LOGIN.EXE will also execute "subscripts" (text files that contain valid script commands). INCLUDE will process a file containing valid login script commands. However, INCLUDE will not display text unless the file contains WRITE commands.

Login script commands are described individually in Appendix A of the *Installation* manual.

What Should a System Login Script Provide?

The basic principle of planning login scripts is to include as much as possible in the system login script. The more a system login script accomplishes, the shorter user login scripts can be.

Some commands are essential in a login script, some are recommended, and others are optional or dependent on the needs of your network.

Essential commands provide access to NetWare and DOS.

- **NetWare utilities.** Use MAP INSERT to map the first search drive to SYS:PUBLIC. This mapping provides access to NetWare utilities (and any programs and batch files you want to store in a public access directory) from any directory.

```
MAP INS S1:=SYS:PUBLIC
```

- **DOS.** Use MAP INSERT to map the second search drive to the DOS directories. This mapping provides access to DOS system files and commands from any directory. When you follow the naming conventions for DOS directories, you can use identifier variables to provide access to the appropriate DOS directory.

  The directory structure you create determines which of the following examples you use.

```
MAP INS S2:=SYS:PUBLIC\V3.30

MAP INS S2:=SYS:PUBLIC\%OS_VERSION

MAP INS S2:=SYS:PUBLIC\%OS\%OS_VERSION

MAP INS S2:=SYS:PUBLIC\%MACHINE\%OS_VERSION

MAP INS S2:=SYS:PUBLIC\%MACHINE\%OS\%OS_VERSION
```

  For guidelines, see **DOS directories.**

- **Command interpreter.** Use COMSPEC to ensure that the transient portion of COMMAND.COM reloads properly into each workstation when an application is exited. COMSPEC should specify the search drive mapped to the DOS directories (in this case, Search2).

```
COMSPEC=S2:COMMAND.COM
```

Recommended commands provide access to frequently used directories. However, to let users know where they are in the directory structure, use [DOS] SET to set the prompt to display the current directory path:

```
SET PROMPT=$P$G
```

- **Application directories.** If an application is used frequently by all or most users, map the next search drive (in numerical order) to the appropriate directory. For example, if all or most users access a word processing program, you could include a search mapping similar to the following.

```
MAP S3:=SYS:APPS/WORDPROC
```

If you have formed groups on the basis of application use, you can assign drive mappings to groups by using the conditional IF...THEN. The conditional IF...THEN is more efficient because it allows you to provide mappings only to users who need them. For example, if only a few of your users need a particular application, you can include a command similar to the following.

```
IF MEMBER OF "WPUSERS" THEN MAP INS S16:=SYS:APPS\WORDPROC
```

When you map a search drive conditionally, consider using Search16, the last possible search drive number. In effect, the system assigns the next search drive available (depending on which search drive numbers have already been assigned). For example, suppose you mapped Search1, Search2, and Search16 (and no others) to directories. If the system cannot find an executable file in Search1 or Search2, the directory mapped to Search16 would be the next directory searched.

As long as you use MAP INSERT, you can map Search16 conditionally to two or more application directories (except in OS/2). Because MAP INSERT inserts a new search drive using the next available number, one mapping will not overwrite another in the following example.

```
IF MEMBER OF "WPUSERS" THEN MAP INS S16:=SYS:APPS\WORDPROC

IF MEMBER OF "SPREADSHEET" THEN MAP INS S16:=SYS:APPS\SS

IF MEMBER OF "DATABASE" THEN MAP INS S16:=SYS:APPS\DBAPP
```

Some applications cannot be run from subdirectories; however, for security reasons, do not assign users rights at the root directory level. NetWare allows you to map a search drive to a fake root (a subdirectory where rights can be assigned to users). To use an application that must be installed at the root, load the files in a subdirectory and include a command in the login script similar to the following.

```
MAP INS ROOT S5:=SYS:APPS\NON_NET_APP
```

- **Home or username directories.** To map the first network drive to each username directory stored in the SYS:HOME directory (or other parent directory), use an identifier variable. The drive mapping would be similar to the following.

```
MAP F:=SYS:HOME/%LOGIN_NAME
```

You can also use a generic drive mapping that maps the first network drive without specifying the drive letter:

```
MAP *1:=SYS:USERS/%LOGIN_NAME
```

To see how to specify drive letters using **n*, see **Directory structure**.

- **Work or database record directories.** To map the second network drive to a directory providing group workspace, use a mapping similar to either of the following.

```
MAP G:=SYS:OFFICE/TRAINING
MAP *2:=SYS:PROJECTS/PLANS
```

- **Common or shareable directories.** To map a drive to a directory used as an intermediate point in transferring files between users, use a mapping similar to the following.

```
MAP H:=SYS:LIMBO
```

Optional commands can include or provide for the following.

- **Messages.** Use WRITE to display a brief message. Enclose the message in quotation marks. Enter identifier variables used within quotation marks as uppercase letters preceded by a percent (%) sign. For example, a message using WRITE commands (including identifier variables) is similar to the following:

```
WRITE "Good %GREETING_TIME, %FULL_NAME."
IF DAY_OF_WEEK = "SUNDAY" THEN WRITE "Why are you working
today?"
```

You can also use FDISPLAY to display longer messages created as text files. All files called up in this way should be in a directory (such as SYS:PUBLIC) to which a search drive has been mapped. Use the PAUSE command after FDISPLAY so that users can read the text before the login script resumes execution. For example, to display a message to members of group SALES, include the following commands.

```
IF MEMBER OF "SALES" THEN FDISPLAY SYS:PUBLIC/SALES.MSG
PAUSE
```

- **Settings for environmental variables.** Use [DOS] SET to set application environmental variables. Generally, if your applications allow for any variable to be set in the DOS environment with SET, you can enter them in the login script. If they apply to all users, include them in the system login script. Any variables that must be set for an individual user should be included in the user's login script.

To determine which variables need to be set, see the documentation that accompanied your application program. Generally, whatever can be set in an AUTOEXEC.BAT file can be set in a login script.

- **Login script batch files.** Use INCLUDE to call up batch files you have created to shorten the login script, to display messages created as text files with WRITE, or to customize the system login script for groups. All files called up in this way should be in a directory to which a search drive has been mapped, such as the SYS:PUBLIC directory or a directory created for batch files, as in the following example.

```
INCLUDE SYS:BATCH/C.BAT
```

- **Additional file servers.** Use ATTACH to access other file servers on an internetwork. When the login script executes, users will be prompted to supply a username for that file server and a password. (You do not access a second set of login scripts when you attach to an additional file server.)

  For example, to provide access to file server ORACLE, include a command similar to the following.

```
ATTACH ORACLE
```

  You can form a group for users who need access to a particular file server, as in the following example.

```
IF MEMBER OF "LEGAL" THEN ATTACH BLACKSTONE
```

  You should also include a drive mapping to the appropriate directory on the additional file server. You must include the name of the file server in the directory path, as in the following.

```
MAP I:= BLACKSTONE/SYS:RESEARCH
```

- **Comments and notes for the network supervisor.** Use REMARK or its aliases, REM, asterisk (*), and semicolon (;), to include explanatory comments so that you have a record of each command's purpose. For example, you might annotate a block of printer mappings with

```
REMARK printer mappings by group

IF MEMBER OF "REPORT1" THEN #CAPTURE Q=PRIORITY ti=3
```

  For an internetwork, you could store each server's login messages in identically named directories and use a standard command similar to the following.

```
;display login messages

FDISPLAY SYS:PUBLIC\NEWS\daily.msg
```

If you use REMARK, the comments and notes are not displayed when the login script executes.

What Should a User Login Script Contain?

For security reasons, each user should have a user login script, however minimal. If you have been able to accomplish your main purposes in the system login script, individual user login scripts need to contain only commands that apply to an individual user. Although you create the initial login script for each user, be aware that users have the right to modify their own login scripts if they are allowed to change their own passwords.

A user login script is similar to a system login script; the same types of commands that are used in the system login script can be used in a user login script. A user login script can contain

- **Drive mappings.** You can map drives to directories frequently used by individual users.

  Do not use the same search drive numbers that you used in the system login script; if you do, the system login script will be overwritten and you will encounter problems with COMSPEC.

- **Environmental variables for applications.** Use [DOS] SET to set application environmental variables that apply to individual users. Whatever can be set in the AUTOEXEC.BAT for a standalone user can be set in the user login script for a network user. (However, you may have to increase environment space in CONFIG.SYS.)

  For example, you can use SET to set environmental variables for the network version of a word processing program. The following command sets a 10-minute backup interval and the user ID (which identifies each user's buffers) for user JSBACH.

```
SET WP = "/b-10/u-jsb/"
```

- **An exit to a menu.** If you want users to work from menus, you can exit to a menu from the user login script. The EXIT command (which terminates the login script) calls up a menu

created for an individual user. You can also combine EXIT with the IF...THEN conditional for menus created for groups. (Do not use EXIT in the system login script; if you do, user login scripts will not be executed.)

Example of a System Login Script

This section provides an example of a system login script. File server AViiON has three volumes: SYS, BOOM, and BAH. The users work at the command line.

The workstations run more than one version of DOS, and two workstations must be able to transfer files to UNIX workstations.

Word processing, office productivity, and electronic mail programs are installed. BOOM is specified as the master volume for mail.

The network supervisor has created daily greeting messages and a monthly reminder to users (introduced with a beep).

The network supervisor also maintains a log file containing login and logout times for users (the Accounting feature is not installed).

```
map display off
dos set mv="aviion/boom:"

map *1:=aviion/sys:
map ins s1:=aviion/sys:public
map ins s2:=aviion/sys:public/%machine/%os_version
comspec = s2:command.com
map ins s3:=aviion/sys:public/wordp-42
rem user-mapped search drives 4-9

rem mappings for mail and office apps
map ins s10:=aviion/boom:mhs/exe
map ins s11:=aviion/boom:atc/exe
map ins s12:=aviion/boom:office
map ins s13:=aviion/boom:wpmail

rem electronic publishing transmission control
protocol
if p_station="0000000000F8" then map ins s4:=c:\pctcp
if p_station="0000000000F7" then map ins s4:=c:\pctcp

map display on

rem daily greeting
if NDAY_OF_WEEK = "1" and hour24 < "09" then
display sys:public/hello1.msg
if NDAY_OF_WEEK = "2" and hour24 < "09" then
```

```
display sys:public/hello2.msg
if NDAY_OF_WEEK = "3" and hour24 < "09" then
display sys:public/hello3.msg
if NDAY_OF_WEEK = "4" and hour24 < "09" then
display sys:public/hello4.msg
if NDAY_OF_WEEK = "5" and hour24 < "09" then
display sys:public/hello5.msg
if NDAY_OF_WEEK = "6" and hour24 < "09" then
display sys:public/hello6.msg
if NDAY_OF_WEEK = "7" and hour24 < "09" then
display sys:public/hello7.msg

rem monthly reminder
if DAY < "07" and NDAY_OF_WEEK = "2" and hour24 < "10"
then begin
 write "\n\7\7 A Monthly Reminder:"
 write "Please delete any unnecessary files you own
 on"
 pause
end

rem user logins
#command /c z:logfil %LOGIN_NAME %P_STATION
%DAY_OF_WEEK %MONTH_NAME %DAY %YEAR %HOUR %MINUTE
%AM_PM
```

Examples of User Login Scripts

This section provides two examples of user login scripts.

Example 1

User JSBACH on file server AViiON has customized this user login script by adding a message and firing phasers at login:

```
set wp = "/b-10/u-jsb/"
set usr = "jsbach"
set pwd = ""
attach ENTERPRISE

MAP INS S5:=ENTERPRISE\SYS:HISTORY\1988
MAP INS S6:=SYS:HOME\JSBACH\MACROS
MAP INS S7:=SYS:PUBLIC\UTIL

#newmail aviion/boom: jsbach

WRITE ""
IF DAY_OF_WEEK = "MONDAY" THEN
WRITE "Sic Transit Gloria Mundi."
WRITE ""
FIRE PHASERS 2 TIMES
```

Example 2

User JAUSTEN on file server AVIION has customized the following user login script by displaying a random quote at login.

```
write ""
write ""

map *4:=boom:print\util
map *5:=bah:humbug

set usr "jausten"
#newmail aviion/boom: jausten
pause
#basica quote
pause
```

Model Login Script for an Internetwork

An MIS staff developed the following model to help network supervisors standardize system login scripts for a large internetwork. The model provides for word processing, accounting programs, and electronic mail.

All file servers in each division begin with the same initial letter. The directory structure is standardized. DOS directories are named in conformity with the pattern in the Search2 mapping. Username directories are in a separate volume named HOME. Accounting work directories are in VOL1. Each database is assigned one or more volumes.

Printer 0 is hard wired and users can print from applications. Other printers require the CAPTURE command.

Advanced users are given access to additional batch files and utilities. A third-party auditing utility is used on most file servers.

```
MAP DISPLAY OFF
WRITE "Good %GREETING_TIME, %FULL_NAME."
WRITE "You are logged onto connection %STATION."

; environment mappings
MAP INS S1: = SYS:PUBLIC
MAP INS S2: = SYS:PUBLIC/%MACHINE/%OS_VERSION
COMSPEC = S2:COMMAND.COM
SET PROMPT = "$P$G"
DOS SET MV = server/SYS:

; personal directory mappings
IF MEMBER OF "HOME" THEN BEGIN
   MAP P: = HOME:\%LOGIN_NAME
   DRIVE P:
END

IF MEMBER OF "HOME2" THEN BEGIN
   MAP P: = HOME2:\%LOGIN_NAME
   DRIVE P:
END

; default printer mappings by group
IF MEMBER OF "PGROUP1" THEN
#CAPTURE Q=PRINTER1 nb nff ti=3

IF MEMBER OF "PGROUP2" THEN
#CAPTURE Q=PRINTER2 nb nff ti=3

IF MEMBER OF "PGROUP3" THEN
#CAPTURE Q=PRINTER3 nb nff ti=3

; mapping required for network applications

; word processing program
IF MEMBER OF "WP42" THEN
MAP S3: = SYS:PUBLIC\WP

IF MEMBER OF "WP50" THEN
MAP S3: = SYS:PUBLIC\WP50

; accounting program
IF MEMBER OF "LOTUS_VI" THEN BEGIN
  MAP INS S16: = SYS:PUBLIC\NET123
  MAP INS S16: = VOL1:USERS\%LOGIN_NAME\123
  MAP O: = SYS:PUBLIC\NET123
  MAP L: = VOL!:USERS\%LOGIN_NAME\123
END

; map miscellaneous search drives
IF MEMBER OF "POWER_USERS" THEN BEGIN
  MAP INS S16: = SYS:PUBLIC\BATCH
  MAP INS S16: = SYS:PUBLIC\UTIL
END
```

```
; supervisor mappings
IF "%LOGIN_NAME" = "supervisor" THEN BEGIN
  MAP P: = SYS:SYSTEM
  MAP *1: = SYS:
  MAP *2: = HOME:
  MAP *3: = HOME2:
  ;etc.
  DRIVE P:
END

; display login messages as required
FDISPLAY SYS:PUBLIC\NEWS\message.txt
PAUSE
WRITE "any short message not in message.txt"
PAUSE

; run miscellaneous programs
#SYS:PUBLIC\lantrail

; display all current drive settings
MAP DISPLAY ON
MAP
```

Long filename

A High Performance File System (HPFS) convention that allows users to label files with long, free-form filenames. Long OS/2 v1.2 filenames can contain embedded spaces, mixed case, and multiple dot delimiters.

For example, an HPFS volume in OS/2 allows filenames of up to 255 characters and path name components up to 260 characters:

Macintosh HPFS volumes allow filenames up to 32 characters.

DOS versions earlier than 5.*x* and older version OS/2 applications allow the following:

- A maximum filename of 12 characters (8 characters, a dot delimiter, and a three-character extension)
- A maximum directory pathname of either 64 or 128 characters, depending on the environment

Long machine type

A six-letter name representing a workstation brand. Use the long machine type in system login scripts to automatically map a drive to the correct version of DOS assigned to the workstation.

IBM computers use the long machine type "IBM_PC." If the workstation is not an IBM computer, you must create a long machine type for the workstation in a SHELL.CFG file.

The six-letter name for the long machine type can also be used as the subdirectory name when you are using more than one brand of workstation on your network. You must use the same six-letter name for DOS directories that you use for the long machine type.

If you are using more than one version of DOS on your network, you must have separate subdirectories for each DOS version used on each machine type.

See also **Directory structure; DOS version.**

LPT1

The primary parallel printer port of a personal computer.

See also **Parallel port.**

LSL

See **Link Support Layer.**

MMM

Macintosh client

A Macintosh computer that attaches to the network. The Macintosh client can store and retrieve data from a NetWare server running Macintosh support modules and can run executable Macintosh network files.

Macintosh clients can share files with DOS and OS/2 clients and can monitor queues.

Servers running NetWare v2.*x* use Macintosh VAPs; Servers running NetWare v3.*x* use Macintosh NLMs; NFAS supports Macintosh clients through the NetWare for Macintosh gateway running on either a NetWare 2.2 server or dedicated router. See also **Client**.

.macres

A file that contains Macintosh resource files to work with NetWare on a host operating system. The Macintosh file system splits information between two files, the data fork and the resource fork. This type of separation is not done under the host file system.

See also ***NWinode* file**.

MAIL directory

The location for electronic mail files. This directory is created during network installation. When users are created, they are assigned a User ID number. (The Supervisor is always given ID number 1; other users are randomly assigned numbers by the file server.) Users are also assigned a subdirectory, or mailbox, in the MAIL directory. The User ID number is used as the mailbox name.

Users are given all rights, except Supervisory, in their mailboxes, but are given only the Create right in the MAIL directory. Each user's login script is stored in his or her mailbox, allowing the login script to be accessed each time the user logs in.

Mapping

The means of assigning a drive letter to a chosen directory path on a volume of a particular file server. For example, if you map drive F: to the directory SYS:ACCTS/RECEIVE, you access that directory every time you enter "F:" at the DOS prompt.

See also **Drive mapping**.

Master workstation diskette

A diskette used to simplify the process of installing numerous workstations on a network. Place the NetWare boot files consisting of LSL.COM, IPXODI.COM, any .CFG files, any DOS boot files, other executable third-party boot files and a shell file (NETX.COM, EMSNETX.EXE, XMSNETX.EXE, or BNETX.COM), on one master diskette. Make copies of this master for each workstation that needs the files for booting (i.e., workstations that have the same type of network board, configuration option, and DOS version).

When you use a master workstation diskette, you save the time it would take to copy each boot file for each workstation with similar boot file requirements.

See also **Boot files**; "Workstation Installation" in the *Installation* manual; *NetWare for DOS* manuals.

Memory board

An add-on board designed to increase the amount of RAM within a personal computer.

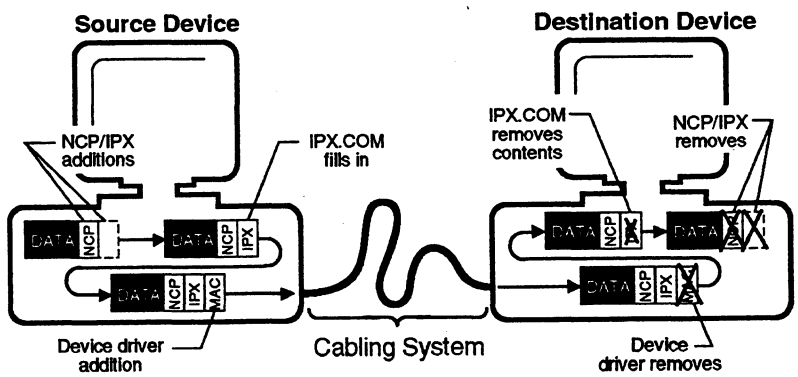
Message

A unit of information used in network communication. Messages sent between network devices (workstations, file servers, etc.) are formed into packets at the source device. The packets are reassembled into complete messages when they reach their destination. A message can contain a request for service, information on how to handle a request, and data that will be serviced.

Each message packet consists of headers and a data portion. The different headers are appended to the data portion as the packet travels through the communication layers. A message that exceeds the maximum size is partitioned and carried as several packets. When the message arrives at its destination, the headers are stripped off each packet in reverse order and the request is serviced.

For example, the NetWare Core Protocol (NCP) attaches a write request header and an IPX header to a piece of data to be written. Then the workstation's IPX communication protocol fills in the IPX header, designating, among other things, the source of the request and the packet length. Finally, the device driver adds a hardware or MAC (Media Access Control) header.

The following figure illustrates a message traveling from a source device to a destination device.



See also **Communication protocols; NCP service protocols.**

Message system

A communications protocol that runs on top of IPX. It provides an engine (process) that allows a node on the network to send messages to other nodes. A set of Application Program Interfaces (APIs) gives programs access to the message system. NetWare supports file server broadcasts and alerts to Supervisors and Workgroup Managers.

Modify right

See **Rights; Security (Rights Security).**

Multiple file server network

See **Multiserver network.**

Multiple-byte characters

Single characters made up of more than one byte. One byte allows 256 different characters. Since the number of ASCII characters equals 256, a computer can handle each ASCII character with one byte. Asian character sets, however, include more than 256 characters; in this case, a computer must use two bytes for each character. NetWare does not support multiple-byte characters.

Multi-link Interface Driver (MLID)

See **LAN driver.**

Multiple name space support

The method that allows various workstations running different operating systems to create their own familiar naming conventions. Multiple name spaces really means that the file system can present multiple client views for any given file.

The name spaces supported on a volume is configurable. (DOS name support is not required.) Each file stored on a given volume has a name that any workstation can recognize. This name is stored in a file entry in the volume's directory table. Different operating systems (DOS, OS/2, Macintosh, UNIX) may have different conventions for naming files. These conventions include name length, legal characters, case-sensitivity or insensitivity, data and resource forks, length of extensions, multiple extensions, and so forth.

For example, a file server configured to support DOS and Macintosh filenames would generate two 128-byte file entries for every file. Volumes that support multiple name spaces use one file/directory entry for each name space supported. The same applies to directory names.

Related utility: *sconsole.*

Multiserver network

A single network that has two or more file servers operating. On a multiserver network, users can access files from any file server to which they are attached (if they have access rights). A multiserver network should not be confused with an internetwork (two or more networks linked together through a router).

See also **Network number.**

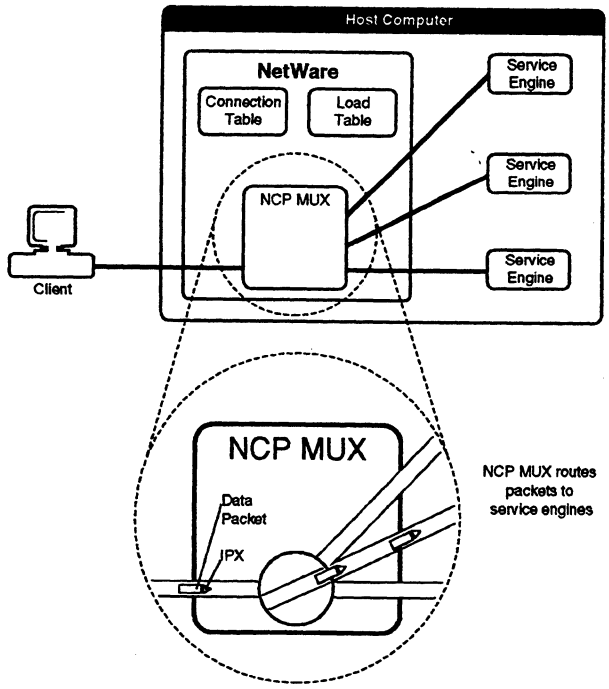
NNN

Name space support

The ability of NetWare to allow workstations running different operating systems to create files using familiar naming conventions and to read files created by other naming conventions. See **Multiple name space support.**

NCP MUX

(NetWare Core Protocol MultipleXer) A host multiplexer for data packets, also known as the NCP driver. The NCP MUX takes packets from IPX and branches them to the service engine assigned to the the client workstation. Depending on the way the service engines are configured, service engines can do work for multiple connections.



NCP MUX consults two tables, the connection table and load table, to determine how to route each packet containing a request for a new connection. The load table shows which service engine has the fewest connections. When a connection request comes in, the NCP MUX picks the least busy service engine and adds that node to the connection table. In the future, requests from that connection always go to the same service engine.

The NCP MUX also decides when to delete a connection.

See also **IPX; Service engine.**

NCP service protocols

(NetWare Core Protocol service protocols) Procedures that a file server's operating system follows to accept and respond to workstation requests.

The process of requesting service from a file server begins in the workstation's RAM where the NetWare shell (NETX.COM, EMSNETX.EXE, XMSNETX.EXE, or BNETX.COM) forms requests according to the definitions of the file server's NetWare Core Protocol.

The shell then hands the requests to the workstation's IPX communication protocol. IPX transmits the request to the file server after attaching a header designating the source and destination. Upon receiving the request, the file server strips off the IPX header and reads the request. Because the NetWare shell has formed the request using the exact guidelines of a specific service protocol, the file server handles the request according to the protocol rules, resulting in a proper response.

NCP service protocols exist for every service a workstation might request from a file server. Common requests handled by the NCP service protocols include creating or destroying a service connection, manipulating directories and files, opening semaphores, altering the bindery (drive mappings and security), and printing.

See also **Communication protocols; IPX; NetWare DOS shell.**

NetBIOS

A NetWare emulation of NetBIOS using SPX that allows workstations to run applications using IBM's NetBIOS calls.

NET.CFG file

A specialized text file created with an ASCII text editor that contains section headings and options that deviate from the defaults of the NetWare shell. NET.CFG files are required when using Novell's LAN Workplace, a third-party protocol, or if you have changed hardware configuration options without using a *PS/2 Reference Diskette.*

See the *NetWare for DOS* manuals.

NetWare Core Protocol

See **NCP service protocol.**

NetWare daemon

An administrative process that runs NetWare on the AViiON system. It does the following when NetWare is booted:

- Reads the *NWConfig* file
- Allocates shared memory
- Opens the STREAMS module (NCP MUX) and links NCP MUX to IPX
- Spawns the service advertiser which communicates with the SAP daemon
- Spawns service engines

The NetWare daemon does the following while NetWare is running:

- Performs watchdog processes
- Manages the pending lock queue
- Manages the events queue

NetWare DOS shell

An interceptor for DOS services that determines whether requests from applications should be sent to DOS or to NetWare. The NetWare DOS shell is loaded into a DOS client workstation's RAM as a Terminate-and-Stay Resident (TSR) program. The shell file and IPXODI.COM are loaded into RAM each time the DOS client workstation is booted. NETX.COM, EMSNETX.EXE, XMSNETX.EXE, and BNETX.COM are NetWare shell files.

The shell is closely linked to other programs and routines creating a larger shell that achieves necessary network communications. If a request needs service on the network, the shell makes the necessary protocol conversions allowing network transmission and destination capture. The shell uses IPX to assign source and destination addresses to a data packet. IPX uses a LAN driver to control transmissions through the network board.

Most requests result in the sending of a single packet to the server, but some calls only provide or manipulate information in the shell's own local tables. The shell initializes several local tables to formulate and track NCP requests. It also builds a table to track connections with file servers (the shell can maintain connections with up to eight servers). Another set of tables is used to track network drives and their mappings, and which file server each network drive refers to.

When an application requests network service, the shell begins the network transmission process at the shell file level. The shell lies between the application layer and DOS, monitoring data transmission. If an application request, such as a call for files, needs to be handled by the file server, the shell file intercepts the request and begins the process of protocol conversion and transmission to the file server.

The shell file intercepts requests by taking over software interrupts 21h (used to call standard DOS functions), 24h (DOS's critical error handler vector), and 17h (used to send data to local printer ports). In general, the shell intercepts all interrupt 21h DOS requests and inspects each one.

After inspection, the shell either passes the request on to the regular DOS interrupt routine or handles it itself. If the shell keeps the request, it converts the request into the NetWare Core Protocol (NCP) and hands it to IPX for transmission to the file server. For data returning from the file server, the conversion of requests is handled in the same fashion but in reverse order. Whether the request is handled by DOS or NetWare is totally transparent to the application and, therefore, to the user.

The NetWare shell file NETX.COM is used when neither an Expanded nor an Extended Memory shell is required. EMSNETX.EXE is used to access expanded memory, and XMSNETX.EXE is used to access extended memory. The file BNETX.COM is a shell file that enables the burst-mode protocol.

See also **Boot files; BNETX.COM; Communication protocols; EMSNET.EXE; IPX; LAN driver; Message packet; NetWare expanded memory shell; NetWare extended memory shell; NET.COM; SPX; XMSNET.EXE.**

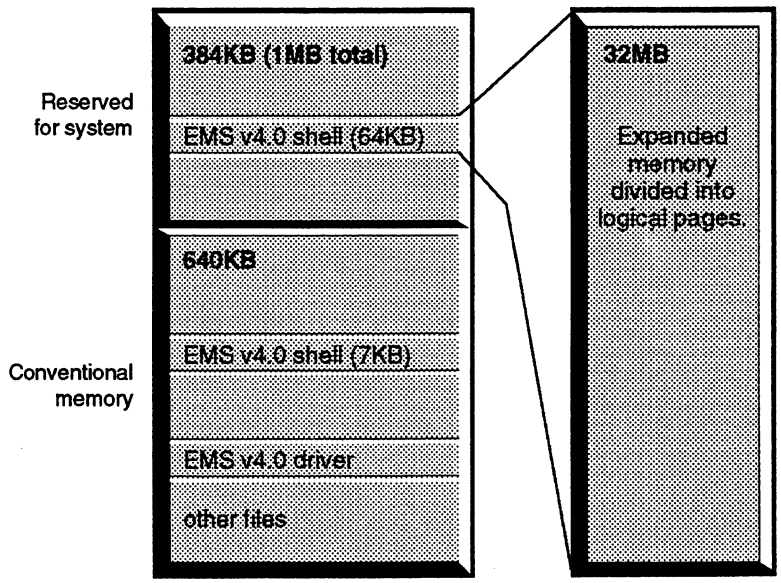
NetWare expanded memory shell

The file NetWare uses to access workstation memory in addition to the 640KB limit of conventional memory. An expanded memory manager swaps memory that exists above the 1MB range into a window, or memory page, below the 1MB range. This allows DOS applications to access up to 32MB of expanded memory.

The NetWare expanded memory shell moves most of the shell out of conventional DOS memory and puts it in expanded memory. This frees up 33KB of memory. The remaining 7KB of the shell must remain in conventional memory to handle interrupts and some data. The NetWare expanded memory shell was written to the specifications of LIM/EMS (Lotus/Intel/Microsoft Expanded Memory Specification) v4.0 memory manager.

Expanded memory manufacturers provide Expanded Memory Specification (EMS)-compatible driver programs. You must load an EMS-compatible driver before loading the NetWare Expanded Memory shell.

To install the NetWare Expanded Memory shell,



- Load a third-party EMS-compatible driver;
- Copy the NetWare Expanded Memory shell file, EMSNETX.EXE, to the workstation boot diskette;
- Include the command EMSNETX.EXE in the AUTOEXEC.BAT file.

Because the Expanded Memory Shell operates in expanded memory, larger applications can run in the conventional memory space. This approach is faster than disk swapping and overlays.

The NetWare Expanded Memory shell works with NetWare v2.1 and above. All the shell configuration (SHELL.CFG) parameters work with the NetWare Expanded Memory shell.

IMPORTANT ⚠

EMSNETX.EXE can only be used with DOS 3.0 and above.

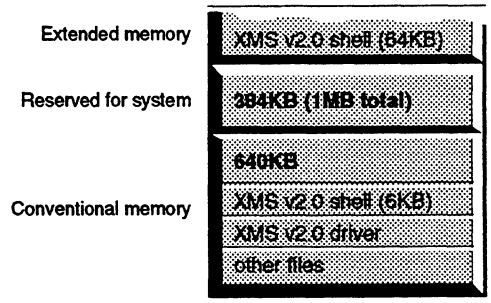
See also **Boot files.**

NetWare Extended Memory shell

The file NetWare uses to access workstation memory above 1MB. Up to 15MB of extended memory are addressable.

The NetWare Extended Memory shell moves most of the shell out of conventional DOS memory and puts it in extended memory. This frees up 34KB of conventional memory. 6KB of the Extended Memory shell must remain in conventional memory to handle interrupts and some data.

The Extended Memory shell requires the support of an XMS (Extended Memory Specification) v2.0 memory manager (or compatible) such as Microsoft's HIMEM.SYS. The memory manager makes the first 64KB (beginning at the 1MB address) of extended memory directly available to DOS-based applications.



To install the NetWare Extended Memory shell,

- Install a third-party extended memory manager;
- Copy the NetWare Extended Memory shell file, XMSNETX.EXE, to the workstation boot disk;
- Include the filename XMSNETX.EXE in the AUTOEXEC.BAT file .

Because the Extended Memory Shell operates in extended memory, larger applications can run in the conventional memory space. This approach is faster than disk swapping and overlays.

The NetWare Extended Memory shell works with all versions of NetWare v2.1x and above.

All the shell configuration (SHELL.CFG) parameters work with the NetWare Extended Memory shell.

IMPORTANT ⚠

XMSNETX.EXE can be used only with DOS 3.0 and above. The current VDISK.SYS from IBM is not compatible with HIMEM.SYS, so do not use the Extended Memory shell with VDISK.SYS.

This shell requires a high degree of IBM compatibility. Depending on the brand of IBM compatible you are using, you may experience keyboard sluggishness or other hardware problems.

See also **Boot files.**

NetWare file system

A file system that allows files from different clients (DOS, Macintosh, OS/2, or UNIX for example) to be stored on the same media. Each client sees the filename in its own native terms: A DOS user sees an eight-character filename with a three-character extension; a Macintosh user sees the multiple-word name. Two clients can access the same file through its native name and modify that file. Do not confuse the NetWare file system with the Network File System (NFS®).

See also **Name space support.**

NetWare Requester for OS/2

Client and peer-to-peer communication software that runs on the OS/2 operating system. The Requester connects OS/2 workstations to NetWare networks, allowing OS/2 users to share network resources with DOS and Macintosh users.

The NetWare Requester for OS/2 also allows application servers (such as SQL server) and their clients to communicate on a network without using a file server. Users can run advanced back-end applications or back-end server engines on their OS/2 workstations. DOS and OS/2 users can then access data on those application servers without using a file server.

When a user or application makes a request to an OS/2 workstation, the request is usually passed to the OS/2 kernel first. The kernel determines whether the request is for local or remote services.

If the request is local (such as printing to a local printer), OS/2 executes it at the workstation. If the request is remote (such as printing to a network printer), the OS/2 kernel passes it to the NetWare Requester for OS/2.

The NetWare Requester determines whether the request is for NetWare services or for Named Pipes. If the request is for NetWare services, the Requester translates it into NetWare Core Protocol (NCP). The NCP request is then passed on to IPX, which uses the LSL to send the information over the network.

If the request is for Named Pipes, the NetWare Requester passes it on to the Named Pipes driver, which delivers the request to SPX without translating it into NCP. SPX then uses the LSL to send the instruction over the network to the correct Named Pipes DOS or OS/2 machine.

See **IPX; Link Support Layer; NCP Service Protocols;** and **SPX.**

NetWare for UNIX

NetWare implemented in a C-language version that is available on host computers. NetWare for AViiON Systems allows NetWare users access to DOS, Macintosh, OS/2, or host operating system applications without modifying the application. The AViiON system can provide fundamental NetWare services (client-server networking). NetWare software runs as a process on the AViiON system.

NetWare routers

See **Routers.**

Network

A group of computers that can communicate with each other, share peripherals (such as hard disks and printers), and access remote hosts or other networks. A NetWare network consists of workstations, peripherals, and one or more file servers. NetWare users can share the same files (both data and program files), send messages directly between individual workstations, and protect files with an extensive security system.

Network address

See **Network number.**

Network board

A circuit board installed in each workstation to allow workstations to communicate with each other and with the file server.

Network communication

Data transmission between workstations. Requests for services and data pass from one workstation to another through a communication medium such as cabling.

Network hard disk

See **Disk.**

Network number

An eight-digit hexadecimal number that uniquely identifies a network. A network is a cabling scheme that connects workstations, servers, and other peripheral equipment. The figures on the following pages use simple network configurations to illustrate the concepts of network numbering. The network numbers used are arbitrary; any combination of hexadecimal numbers in the range of 1 to FFFFFFFE are valid network addresses. For simplicity, the illustrations use a bus topology; however, the concepts presented apply to any network topology.

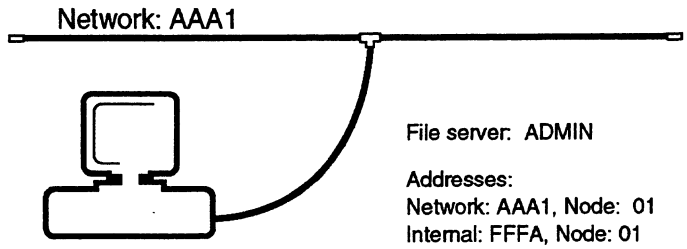
Network numbering concepts can be compared to a postal numbering system. A street number (or name) identifies a city street, and building numbers identify individual buildings along the street. The combination of a street number (or name) and a building number tells the post office where to deliver mail within a city.

A network address identifies a network cabling scheme, and node numbers identify individual workstations along the network cable. Data is distributed on a network in envelopes called *packets* (or *frames*). Each packet is stamped with a source and a destination address. Both the source and destination addresses consist of a network address and a node number.

Thus a network is a single cabling scheme identified by a unique address to which one or more workstations are attached, each of which are identified by numbers that are unique along the network.

Single server network

The following figure shows a simple network configuration—one server attached to one network. In this configuration, the network number AAA1 identifies the network to which server ADMIN is attached.

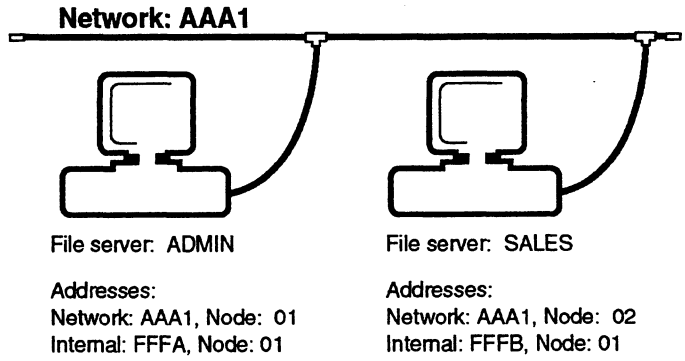


Server ADMIN uses the network number FFFA to identify the internal network. An internal network number is a feature of NetWare v3.*x*. An internal network number is a *logical* network that routes packets to the physical networks to which a file server is attached.

The node number 1 distinguishes server ADMIN from any other workstation on network AAA1. The operating system assigns the node number of 1 to the internal network.

Multiserver network

The following figure illustrates the first configuration slightly expanded by the addition of a second server, SALES, to the same network. This configuration is called a multiserver network.

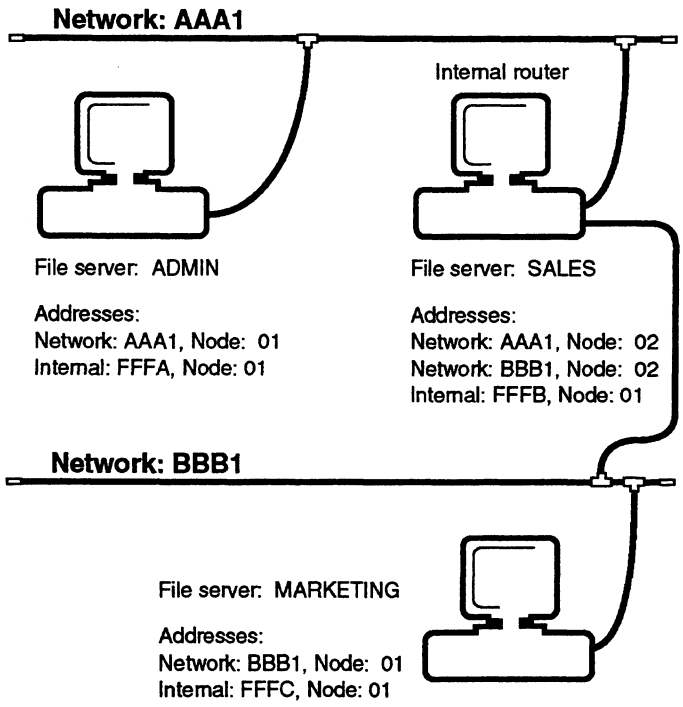


SALES and ADMIN share the same physical network number AAA1. However, because node numbers must be unique within each network, each server uses a different node number on network AAA1.

Because both servers see each internal network as a separate network, the internal networks must use unique network numbers. In this configuration, the server SALES uses the internal network number FFFB.

Multiserver internetwork

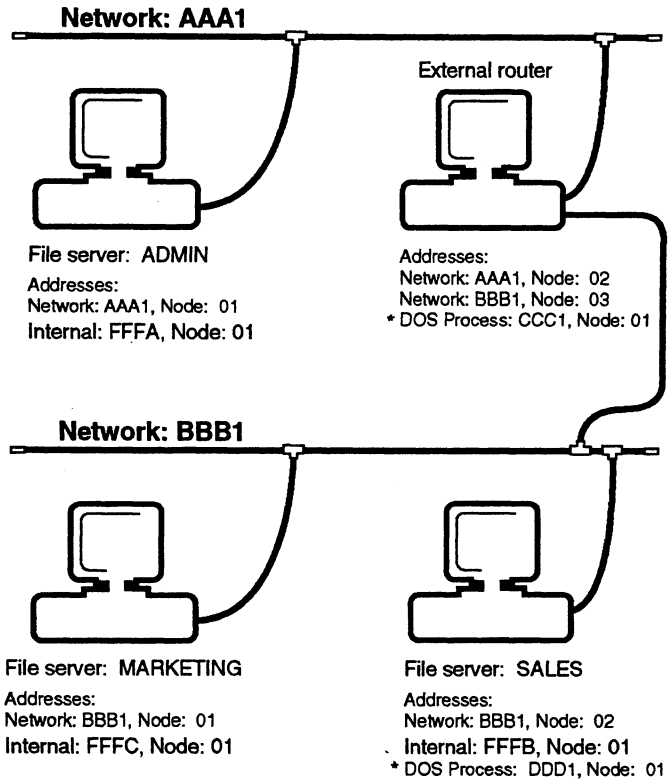
The following figure shows the configuration with a second network. This is a multiserver internetwork. An internetwork is a series of two or more networks linked through internal or external routers.



On an internetwork, workstations on a network can communicate with workstations on other networks. In this internetwork, server SALES performs the function of an internal router. This means that server SALES routes data frames between networks AAA1 and BBB1.

The configuration includes a third server, MARKETING. Because server SALES is attached to both networks AAA1 and BBB1, all three servers can communicate with each other.

The following figure illustrates an internetwork that uses an external router between the networks AAA1 and BBB1.



* Used with nondedicated file servers and routers

The external router in the previous figure performs the same functions as server SALES in the previous figure. However, routing data packets between networks is the main function of the external routers. Therefore, server SALES in the above figure is relieved from the task of routing data packets between different networks. In this internetwork, the external router performs the routing services between the networks AAA1 and BBB1.

The external router function is similar to that of server SALES in the figure on the previous page except the router is configured as nondedicated. A nondedicated router can also function as a workstation. Because the router is configured as a nondedicated router, the router's operating system uses a nondedicated DOS process.

A nondedicated DOS process is a special-purpose router used in the operating systems of nondedicated routers and file servers. Like the internal network of a NetWare server, a nondedicated DOS process is a logical network. However, this logical network has only one workstation attached: the workstation function of the router. The router operating system treats this workstation function of the router as a logical workstation.

This nondedicated DOS process routes data packets from the logical workstation of the router to the router's operating system. Because a nondedicated DOS process is a logical network, it must be assigned a network number that is unique to the number of the network to which the router is attached. This number must also be unique on the internetwork. In a nondedicated file server or router, the logical workstation is assigned node number 1 and the router station number is assigned node number 2.

The configuration in the preceding figure also includes server MARKETING. Because server MARKETING is attached to the network BBB1, the router of server MARKETING must use the network number BBB1 and a node number unique to network BBB1.

Network operator

See **User.**

Network station

A personal computer connected to a network by means of a network board and a communication medium. A network station can be either a workstation or a router.

Network supervisor

See **SUPERVISOR; User.**

NETX.COM file

The NetWare shell program that works with IPX, SPX, and a LAN driver to convert a standalone computer into a workstation. Loaded into RAM each time a workstation boots, NETX begins network transmission each time a workstation requires service on the network. (Other NetWare shells are EMSNETX.EXE, XMSNETX.EXE, and BNETX.COM.)

The NETX program lies on top of the workstation operating system, between the application layer and DOS. NETX monitors all data transmission moving in or out of DOS or the application layer. If an application request, such as a call for files, needs to be handled by the file server, NETX intercepts the request and begins protocol conversion and transmission to the file server.

NETX intercepts requests by taking over software interrupts 21h (used to call standard DOS functions), 24h (DOS's critical error handler vector) and 17h (used to send data to local printer ports).

In general, the shell intercepts all interrupt 21h DOS requests and inspects each one. After inspection, the shell either passes the request on to the regular DOS interrupt routine or handles the request itself. If the shell keeps the request, it converts the request into the NetWare Core Protocol and hands it to IPX for transmission to the file server. For data returning from the file server, the conversion of requests is handled in the same fashion but in reverse order. Whether the request is handled by DOS or NetWare, it is totally transparent to the application and, therefore, to the user.

See also **BNETX.COM; EMSNETX.EXE; IPX; LAN driver; NetWare DOS shell; SPX; XMSNETX.EXE.**

Node address

See **Network number.**

Node number

A number that identifies a network station. Every station on a network has a unique node number to distinguish it from other stations.

See also **Network number.**

Novell Virtual Terminal

See **NVT.**

NPSConfig

A configuration file that the NPS daemon uses to establish the NetWare protocol environment.

NPSConfig contains parameters to:

- Activate IPX
- Activate SPX
- Activate NetBIOS
- Activate NVT
- Identify the network numbers for each file server network board
- Identify the internal network number
- Load the Ethernet and/or Token Ring drivers
- Load the SHIM module
- Idenfify NVT configurations

See also the *System Administration* manual.

NPS daemon

(NetWare Protocol Stack daemon) An administrative process that opens up the STREAMS modules and holds them open while the NetWare transports are running.

The NPS daemon determines the configuration to build from the NSPConfig file. The NPS daemon then initializes the SAP daemon.

See also **NPSConfig; NWConfig**

NVT

(Novell Virtual Terminal) A TSR program on the client and a driver on the AViiON computer that allow personal computers to establish a virtual terminal session with an AViiON system host running NetWare transport protocols. This feature gives users access to DG/UX applications.

NVT is compatible with almost all third-party terminal emulation software that runs on PCs. The DOS client workstations load IPX, NVT and third-party terminal emulation software.

The AViiON system host has the NPS daemon initialized and has activated both SAP and NVT STREAMS.

Related utilities: **IPX, NVT** in *Utilities; **sconsole*** in *System Administration.*

NWConfig

A host configuration file for the NetWare daemon. The NetWare daemon reads NWConfig to establish the NetWare environment. NWConfig contains over 50 parameters to set with *sconsole.*

The mandatory parameters are the file server name and the volume SYS assignment (the path to the NetWare logical root). Volume SYS contains the NetWare public files and system files.

Other often-used parameters are:

- Total connections allowed on the file server
- Connections allowed per service engine
- Total number of service engines
- Whether to allow hybrid users

See also **NetWare daemon**; the *System Administration* manual.

NWinode file

A file that stores all NetWare information about data files stored in a NetWare volume on the host directory structure. This is information specific to NetWare files that is not kept by the DG/UX operating system.

When a client writes a file out to the host, the host actually writes to two files. The first file is the actual data file. The second one is the inode file. It contains information such as the filename, modification time, access time, the NetWare owner ID, and name space information. See also **Attributes**.

OOO

Object

An entity defined on the network and with access to the file server. Object types include users, groups, file servers, print servers, and backup servers and are defined in the file server's bindery.

See also **Bindery.**

ODI

(Open Data-Link Interface) A standard interface that allows transport protocols to share a single network board without conflict. ODI supports media- and protocol-independent communications by allowing the user to link any combination of LAN drivers to protocols. See the *NetWare for DOS* manuals.

See also **Dedicated IPX drivers; NetWare DOS shell.**

Open Data-Link Interface

See **ODI.**

OS/2 Client

OS/2 software that connects to the network using NetWare Requester software. The OS/2 client can store and retrieve data from the network service engine and run executable network files. OS/2 client workstations now include IPX/SPX and NetBIOS support to allow DOS users access to OS/2-based applications such as the SQL Server. See **NetWare Requester for OS/2.**

OS/2 Requester

See **NetWare Requester for OS/2.**

PPP

Packet

See **Message packet.**

Parallel port

An interface that allows data to be transmitted a byte at a time, all eight bits moving in parallel.

See also **LPT1.**

Parent directory

The directory immediately above any subdirectory. For example, SYS:ACCTS would be the parent directory of the subdirectory SYS:ACCTS/RECEIVE.

See also **Directory structure.**

Parity

See **Serial communication.**

Partitions

Logical divisions of hard disks. The host operating system's hard disks can be logically partitioned, so that they appear as separate devices or one device.

See also **Data protection; Host file system; Volume.**

Passive hub

A device used in certain network topologies to split a transmission signal, allowing additional workstations to be added. A passive hub cannot amplify the signal, so it must be connected directly to a workstation or an active hub.

See also **Active hub**.

Password

The word a user must know to log in, if a password is required. NetWare gives you the option to assign a login password to each user. If passwords are required, each user must have a password. The supervisor can determine whether these passwords must be unique or not. In NetWare v3.*x*, login passwords are encrypted at the workstation and put into a format that only the file server can decode. This format prevents intruders from accessing files.

Passwords in NetWare versions below 2.15 Rev. C, however, are sent across the network in a clear text format. A packet analyzer can pull in a login packet that uses the clear text format, and an intruder can read a user's login password.

See also **Security (Login Security); User; User account.**

Path

A variable that appears in command formats. *Path* represents a NetWare directory path that includes the file server, volume, directory, subdirectory, or file you need in your command. Replace *path* by typing the drive letter or the complete directory path.

See also **Directory structure.**

Port, hardware

A connecting component that allows a microprocessor to communicate with a compatible peripheral.

See also **Parallel port; Serial port.**

Port, software

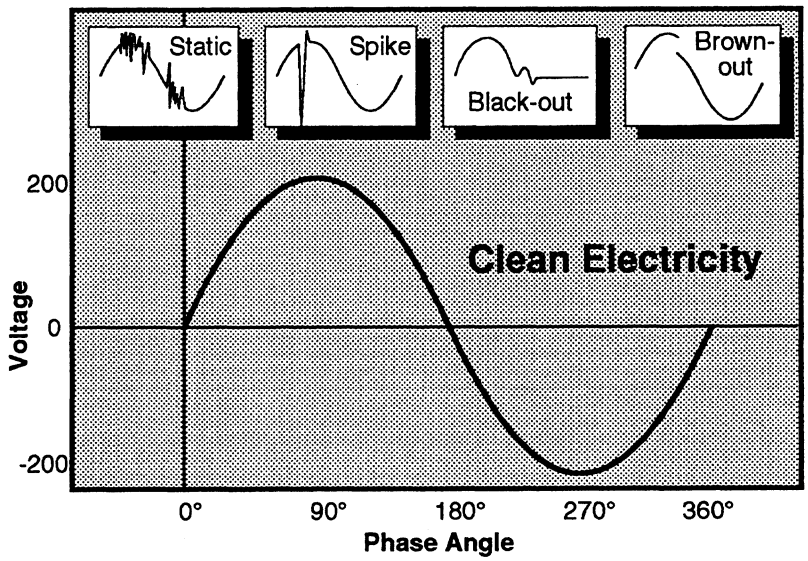
A memory address that identifies the physical circuit used to transfer information between a microprocessor and a peripheral.

Power conditioning

A means of avoiding power fluctuations that disrupt or destroy the network. Because network hardware components are sensitive to power fluctuations, all power lines connected to such components should use power conditioning equipment.

Electricity, as it leaves a commercial power facility, is very clean. In fact, most companies spend a high percentage of resources to make sure the power they put out is a pure sine wave. Unfortunately, nearly all devices create disturbances that pollute the sine wave. As power travels though a wire away from the power plant, it picks up more of these interferences. Effective power conditioning requires an understanding of how these disturbances affect the standard Alternating Current (AC) sine wave.

A pure AC power sine wave appears as the smooth wave in the following figure. The height of the wave is measured in voltage. The wave starts at zero volts and moves to the highest point of 120 volts. The wave eventually cycles through a low point of -120 volts and back to zero. The speed at which it travels through this cycle is the frequency. Normal power cycles at about 60 times per second. Anything that disrupts this wave can cause hardware or data problems and needs to be regulated.



Power disturbances can be categorized in several ways. A transient, sometimes called a spike or surge, is a very short but extreme burst of voltage. Noise or static is a smaller change in voltage. Brownouts and blackouts are the temporary drop or loss in electrical power. To protect equipment from each of these events, three types of protection are available: suppression, isolation, and regulation. The supervisor should verify that the appropriate combination of these three types of protection is properly installed for each installation.

Suppression protects against transients. The most common suppression devices are surge protectors. Surge protectors usually have circuitry that prevents excess voltage. Though manufacturers originally designed surge protectors to prevent large voltage changes, most also have added circuitry to reduce noise on the line.

Isolation is the method used to protect against noise. Ferro-resonant isolation transformers use a transformer within the circuitry to envelop the sine wave at a slightly higher and lower voltage. Any voltage irregularity that extends beyond this envelope is clamped. Isolation transformers are usually very expensive.

Regulation means to modify the power wave to conform to a nearly pure wave form. The Uninterruptible Power Supply (UPS) is the most commonly used form of regulation. A UPS comes in two varieties, on-line and off-line.

An on-line UPS actively modifies the power as it moves through the unit. This is closer to true regulation than the off-line variety. If a power outage occurs, the unit is already active and continues to provide power. The on-line UPS is usually more expensive but provides a nearly constant source of energy during power outage.

An off-line UPS monitors the AC line; then, when power drops, it activates. The drawback to this method is the slight lag before the off-line UPS activates. Most commercial systems are fast enough to compensate for any delays, however.

Because having a UPS tied to every workstation is expensive, most companies attach only the most critical devices, such as file servers, routers, and hard disk subsystems, to the UPS. However, because most programs run on the workstation, data stored in RAM is not saved during a power outage. The reason for placing the UPS on a file server is to enable the file server to properly close files and rewrite the system directory to disk. If the UPS doesn't have its own form of surge protection, it is a good idea to protect the UPS from transients using a surge protector.

Proper use of power conditioning devices greatly reduces the maintenance costs of a network. Make sure that the proper amount of amperage is available for each system and that all outlets are grounded. Dedicated power lines provide ample amperage. Power conditioning devices connected to poorly grounded outlets do very little in protecting your hardware.

Studies have shown that total network maintenance costs are higher with line-surge suppressors and ferro-resonant isolation transformers alone than with uninterruptible power supplies.

Print device

A printer, plotter, or other peripheral used to produce hard copy.

See also **Printing**.

Print function

A printer command that determines the characteristics of a print job. For example, a print function can specify the style of typeface.

Print job configuration

A group of characteristics that determine how a job is printed. The characteristics may include the mode, the form, the number of copies, and the particular printer used. Users can create print job configurations using the PRINTCON utility.

See also **Print mode**.

Print mode

A sequence of print functions that determines the appearance of the printed output. A print mode can define the style, size, boldness, and orientation of the typeface. SUPERVISOR uses PRINTDEF to designate print modes, allowing users to quickly select a combination of print functions.

Print queue

Subdirectories in NetWare's SYS:SYSTEM directory that store print jobs waiting to be serviced by the host's print services. A print job arrives in the queue after being printed to a file (spooled) for temporary queue storage.

Host print services are attached to the file server queue and move the queued print jobs to the host printer. The order in which the print jobs go to the printer depends on NetWare's queue management program and the host printing services tied into that queue.

Queue management arranges print jobs in a queue according to the time they arrive, which usually means they are printed on a first in/first out basis. Users can set print file holds and timed releases on a job, and a queue operator can change the sequence of the jobs waiting in the queue. Queue management tracks the status of queued jobs, releasing them to the host at the proper time, in the proper order.

See **Print server**.

Print queue operator

A printing supervisor with rights to create, manage, disable, and enable print queues. A print queue operator can also authorize a print server to service a queue. The SUPERVISOR is print queue operator by default; however, the SUPERVISOR can delegate this responsibility to another user using the PCONSOLE utility (*Utilities* manual).

Print server

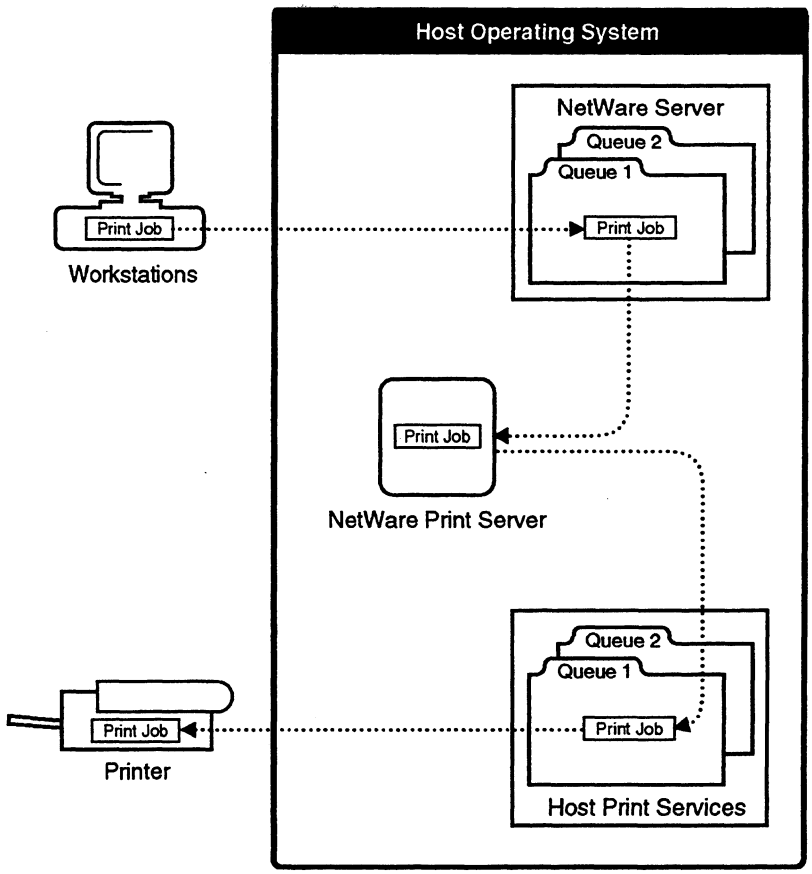
A service process that resides on the AViiON or on a dedicated microcomputer. When a user on a network sends a print job to a network printer, the job is routed to a print queue on the file server. The queue stores the job until the print server can deliver it to the printer. When the printer is available, the print server sends the job to the printer.

Each native NetWare print server supports up to sixteen printers; a pserver daemon on the AViiON system supports up to 64 printers. The print server allows you to physically locate printers where you need them, not just next to the file server.

With NetWare on an AViiON, the print queues can be serviced by any version of the print server (NLM, VAP, or DOS .EXE). They can also be serviced by the PSERVER daemon. The PSERVER daemon runs as a process on the AViiON. Only remote printers can attach to the PSERVER daemon. If the remote printer (the RPRINTER daemon) is initialized on the host, RPRINTER can be configured to spool the print jobs from the NetWare print queues to DG/UX print queues. Host printers will then print the jobs.

You can start and stop the PSERVER and RPRINTER daemons from *sconsole*.

NetWare's printing utilities (CAPTURE, NPRINT, and PCONSOLE) attach a header to your files containing printer-specific commands which tell the printer how to print the entire file. These printer commands include the number of copies, banner page information, and printer commands you choose for your printer. To reset your printer after printing, select a reset command and NetWare will attach it to the end of your file.



Define customized printer commands with PRINTCON and PRINTDEF and use them with CAPTURE, NPRINT, and PCONSOLE.

See the *Print Server* manual.

Print server operator

A printing supervisor with rights in PCONSOLE for the following:

- Attach to other file servers
- Specify who to notify if the printer needs service
- Issue commands to the printer

- Change forms for the printer
- Change the queues serviced by a print server
- Change queue priority
- Down the print server

A print server operator cannot create new print servers or assign other users as print server operators.

The SUPERVISOR is a print server operator by default; however, the SUPERVISOR may assign another user as print server operator by using the PCONSOLE utility (*Utilities* manual).

To establish the proper connection between the print server and the print queue, a user must be both print server operator and print queue operator, or enlist the help of the print queue operator of each queue serviced by the print server.

See also **Print server; Print spooling.**

Related utility: **PCONSOLE** (*Utilities* manual).

Print spooling

A process that prints to a file rather than printing to a printer (or local printer port). NetWare-compatible applications prepare the file to be printed by making sure the file contains only the data to be printed and printer-specific commands. This file is different than the original file which usually contains application-specific commands and characters that are unprintable.

NetWare-compatible applications spool all print jobs to a file server queue. If you use an application that is unable to spool, you can print your files to a local port and use CAPTURE to reroute the file to a queue where it, in effect, becomes a spooled file. If you use an application that can spool to a file but does not recognize network queues, you can spool to a file and then queue the file with NPRINT and PCONSOLE.

Once a queue has been created, use the host-based *sconsole* utility to select a host printing service and to connect the queue to that service.

See the *Print Server* manual.

Print utilities

NetWare programs that can affect where the print job is sent, who can control it, and what happens to it at the printer. Use NetWare utilities to print with applications unable to spool files, print from disks, and print screen displays.

If you usually print with a network-compatible application, you will seldom need to use the NetWare print utilities except to set up and monitor your print process.

Printing tasks are handled by the following NetWare print utilities.

TASK	UTILITY
Setup	PCONSOLE, *sconsole*
Special Printer Instructions	PRINTDEF, PRINTCON
Printing	CAPTURE, NPRINT, PCONSOLE
Control Queued Files	PCONSOLE

Process

A systematic sequence of operations that transforms raw data into useful information. In a NetWare context, process is synonymous with engine.

Each user that logs in to NetWare is assigned to a process. Rather than creating or spawning a new process every time a user logs in, NetWare automatically spawns extra processes so that they are available whenever a user needs one. When a user ends a connection, either by rebooting or by logging in to another file server, that connection to the process is eliminated.

The supervisor sets the maximum number of processes to run. Each process can have a number of clients. At first, as users log in, each gets a process. Once the maximum number of processes is used, clients are stacked within a process. Client stacking can eventually degrade performance.

See also **Client; NWConfig; Service engine.**

Prompt

A character or message (generated by the software) that appears on the display screen and requires a response (such as a command or a utility name) from the user.

Standard types of prompts include

- The DOS prompt, which displays one of the local drives (A to E) followed by a caret: A>
- The network prompt, which displays one of the network drives (F to Z) followed by a caret: F>
- The file server console prompt, which displays a colon
- The OS/2 prompt, which displays a drive letter in brackets: [B]

Property

A descriptive feature of a bindery object such as a password, account restriction, account balance, internetwork address, or list of authorized clients.

See also **Bindery; Object.**

Protocol

See **NCP service protocols.**

Protocol, NetWare Core

See **NCP service protocols.**

Public access

A security condition that gives all NetWare users access rights to a particular directory. For example, all NetWare users must be able to access NetWare utilities. Therefore, NetWare utilities are usually placed in a directory (named SYS:PUBLIC) that has public access rights; in other words, all users have File Scan and Read rights for files in that directory.

PUBLIC directory

The location where NetWare utilities, as well as the .OVL and .DAT files necessary to run the menu utilities, are copied into the PUBLIC directory during installation. All NetWare users have a search drive mapped to the PUBLIC directory through the system login script and are assigned Read and File Scan rights to this directory.

Public files

Files that need to be accessed by all NetWare users. By convention, they are located in the SYS:PUBLIC directory. This general access directory is created during network installation and cannot be deleted. NetWare utilities, help files, and some message and data files (such as the system login script file, NET$LOG.DAT) are public files that all NetWare users have File Scan and Read rights to.

Purge attribute

See **Attributes; Security (Attribute Security).**

QQQ

Queue

See **Print queue.**

RRR

RAM buffer address

See **Base memory address.**

Read Audit attribute

See **Attributes; Security (Attribute Security).**

Read Only attribute

See **Attributes; Security (Attribute Security).**

Read right

See **Rights; Security (Rights Security).**

Read Write attribute

See **Attributes; Security (Attribute Security).**

Record locking

A feature of NetWare that prevents different users from gaining simultaneous access to the same record in a shared file, thus preventing overlapping disk writes and ensuring data integrity.

Recursive copying

The process of copying a specified source directory to a destination directory until all the files and subdirectories in and below the specified source directory are copied.

Recursive copying copies all directories and files of a logical drive to the destination, keeping them exactly as they were in the source directory. Whether a trustee's rights are copied with the files and directories depends on what rights are assigned in the destination directory. The DOS XCOPY, NCOPY, and BACKUP utilities use recursive copying.

Remote boot

The method of booting a workstation from remote boot image files on a file server rather than from a boot diskette in the workstation's local drive. When a workstation is booted, the Remote Reset PROM (installed on the workstation's network board) directs the nearest (default) file server to run the remote boot image file commands contained in the default server's SYS:LOGIN directory.

See also **Remote Reset.**

Remote connection

A connection between a LAN and a workstation or network, often using telephone lines. A remote connection allows data to be sent and received across greater distances than those allowed by normal cabling.

Remote Reset

A program that allows you to boot a workstation from remote boot image files on a file server rather than from a boot diskette in the workstation's local drive. Before you can use Remote Reset, you must install a PROM on the workstation's network board and run the DOSGEN utility (see Appendix D: "Using DOSGEN to add Remote Reset" in the *Installation* manual.)

DOSGEN uploads a workstation's boot files into an image file on the file server. The AUTOEXEC.BAT file is included in the image file and is used by a workstation just as if the file were present on a local boot diskette. However, the workstation boot process (using Remote Reset) requires the AUTOEXEC.BAT file to be copied not only to the image file, but also to the SYS:LOGIN directory and any default directory named in the workstation's login script.

When the workstation boots, the Remote Reset PROM directs the operating system to search for boot files on a diskette in drive A. If boot files are found in drive A, the PROM shuts down and allows drive A to load the boot files. If the files are not found, the system looks for files on a local hard disk. If boot files exist on the local hard disk, the system asks whether you want to shut down the PROM and boot from the local hard disk, or let the PROM boot from the network. If boot files are not found on the local hard disk, the PROM connects to the file server's SYS:LOGIN directory and runs the boot file commands contained in the remote boot image file.

NOTE 

Whether the operating system finds the boot files in drive A, drive C, or through the PROM in the SYS:LOGIN directory, the system still assumes it is reading the boot files from drive A.

When an AUTOEXEC.BAT file instructs the operating system to load the shell file (NETX.COM, for example) the connection to the image file is ended and the shell makes a new connection to the SYS:LOGIN directory. The system then returns to drive A to complete the AUTOEXEC.BAT commands.

Since the AUTOEXEC.BAT file is not in drive A, the system is unable to complete the batch file commands there. The operating system continues with the batch file commands from the AUTOEXEC.BAT file in the SYS:LOGIN directory.

If a user's login script maps to a default directory other than SYS:LOGIN, the system terminates the connection with the AUTOEXEC.BAT file as it leaves the SYS:LOGIN directory and moves to the new directory. The system completes any remaining batch file commands, from the AUTOEXEC.BAT file in the default directory.

Multiple AUTOEXEC.BAT files. With multiple remote boot image files, a workstation's operating system first looks in a BOOTCONF.SYS file to find out which image file it uses. The system then goes to that image file and runs the commands listed in the AUTOEXEC.BAT file.

As described earlier, the boot process needs that batch file copied into the SYS:LOGIN directory as well as any default directory named in a login script. But with multiple remote boot image files, multiple AUTOEXEC.BAT files need to be copied. Since a directory can contain only one file with a particular name, each AUTOEXEC.BAT file is renamed (usually to the user's name with a .BAT extension) before it is copied.

But when the operating system first uses the image file, it looks for executable commands in an AUTOEXEC.BAT file.

With multiple batch files to boot each user's workstation, another batch file (named AUTOEXEC.BAT) contains one command: the newly renamed batch file. This AUTOEXEC.BAT file directs the system to use the renamed batch file for all subsequent batch file commands.

See also **Boot files.**

Remote workstation

A terminal or personal computer connected to the LAN by a router or through a remote asynchronous connection. A remote workstation can be either a standalone computer or a workstation on another network.

Rename Inhibit attribute

See **Attributes; Security (Attribute Security).**

Resource

In NetWare installation programs, a device, feature, circuit board, or built-in circuitry that uses one or more of the following to communicate with the file server's microprocessor: interrupt lines, DMA lines, I/O addresses, or memory addresses (RAM or ROM).

Rights

The method of controlling which directories and files a user can access and what the user is allowed to do with those directories and files.

Eight rights can be granted at either the directory or file level: Access Control, Create, Erase, File Scan, Modify, Read, Supervisory, and Write. Rights granted at the directory level can be redefined for a file by making new trustee assignments or revoking rights from the Inherited Rights Masks.

SUPERVISOR has all rights and grants trustee assignments to users and groups. When users are created, they become a member of group EVERYONE and obtain all rights granted to that group.

Users are granted the right to search to the root of a directory whenever they are granted any rights to a directory or file. They cannot see subdirectories unless they are granted rights to the subdirectories or to files in the subdirectories.

- **Access Control right** allows users to modify trustee assignments and Inherited Rights Masks.

Access Control Rights

	Directory Level	File Level
Directory Trustee Assignments	Modify	No rights
File Trustee Assignments	Modify	Modify
Inherited Rights Mask	Modify	Modify
Rights	Grant any (except Supervisory)	Grant any (except Supervisory)

Use the letter **A** to represent this right.

Related utilities: **ALLOW; FILER; GRANT; REVOKE; RIGHTS; SYSCON** (*Utilities*).

- **Create right** allows users to create directories and files. At the directory level, this right allows users to create files and subdirectories in the directory.

  If users are granted only the Create right at the directory level and no rights below the directory, this right creates a drop box directory. In a drop box directory, users can create a file, and then open and write to the file. Once the file is closed, however, they cannot see or modify the file. They can also copy files and subdirectories into the directory. When they copy, they assume ownership of the files and subdirectories. However, any trustee assignments assigned to the files or subdirectories are revoked.

  Use the letter **C** to represent this right.

  Related utilities: **ALLOW; FILER; GRANT; REVOKE; RIGHTS; SYSCON** (*Utilities.*)

- **Erase right** allows users to delete directories and files. At the directory level, this right allows users to delete a directory as well as files, subdirectories, and subdirectory files in that directory. At the file level, this right allows users to delete the file (even when the right has been revoked at the directory level).

  Use the letter **E** to represent this right.

  Related utilities: **ALLOW; FILER; GRANT; REVOKE; RIGHTS; SYSCON** (*Utilities.*)

- **File Scan right** allows users to see files. At the directory level, this right allows users to see files and subdirectories in a directory. At the file level, this right allows users to see the file (even when the right has been revoked at the directory level).

  Use the letter **F** to represent this right.

  Related utilities: **ALLOW; FILER; GRANT; REVOKE; RIGHTS; SYSCON** (*Utilities.*)

- **Modify right** allows users to change directory and file attributes and to rename subdirectories and files. At the directory level, this right allows users to change the attributes of and rename any file, subdirectory, or subdirectory file in that directory. At the file level, this right allows users to change the file's attributes or to rename the file (even when the right has been revoked at the directory level).

  Use the letter **M** to represent this right.

  Related utilities: **ALLOW; FILER; GRANT; REVOKE; RIGHTS; SYSCON** (*Utilities*).

- **Read right** allows users to open and read files. At the directory level, this right allows users to open files in a directory and read the contents or run the program. At the file level, this right allows users to open and read the file (even when the right has been revoked at the directory level).

  Use the letter **R** to represent this right.

  Related utilities: **ALLOW; FILER; GRANT; REVOKE; RIGHTS; SYSCON** (*Utilities*).

- **Supervisory right** grants all rights to the directory or file. At the directory level, this right grants all rights to the directory and to files, subdirectories, or subdirectory files in that directory. The Supervisory right overrides restrictions placed on subdirectories or files with Inherited Rights Masks. Users who have the Supervisory right in a directory can grant other users Supervisory rights to the directory, its files, and subdirectories.

  Once the Supervisory right has been granted, it can be revoked only from the directory it was granted to. It cannot be revoked in a file or subdirectory.

  At the file level, this right grants all rights to the file. Users who have this right can grant any file right to another user and can modify all rights in the file's Inherited Rights Mask.

  Use the letter **S** to represent this right.

  Related utilities: **ALLOW; FILER; GRANT; REVOKE; RIGHTS; SYSCON** (*Utilities*).

- **Write right** allows users to write to files. At the directory level, this right allows users to open and write to (modify the contents of) files in the directory. At the file level, this right allows users to open and write to the file (even if the right has been revoked at the directory level).

  Use the letter **W** to represent this right.

  Related utilities: **ALLOW; FILER; GRANT; REVOKE; RIGHTS; SYSCON** (*Utilities*).

See also **Inherited Rights Mask; Security (Rights Security).**

RIP

See **Router Information Protocol.**

Root

A superuser in the DG/UX operating system who has access to everything.

Root directory

The highest directory level in a hierarchical directory structure. With NetWare, the root directory is the volume; all other directories are subdirectories of the volume.

See also **Directory structure; Fake Root.**

Root file system

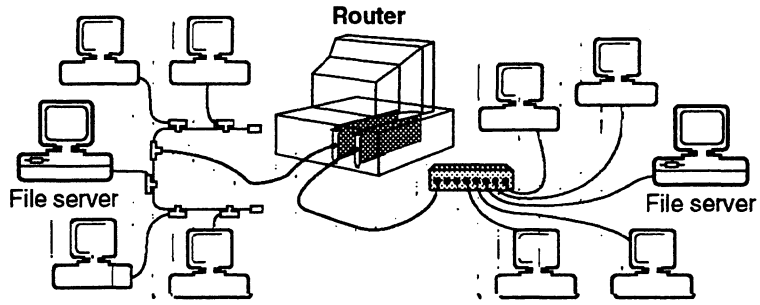
Contains the programs necessary to boot the operating system, create a hierarchy of file systems, and repair the file systems, including the root file system itself. DOS file systems contain one root directory per volume. DG/UX file systems contain a single root directory which allows partitions to be spliced in. All filesystem objects vary depending on the operating system.

Router

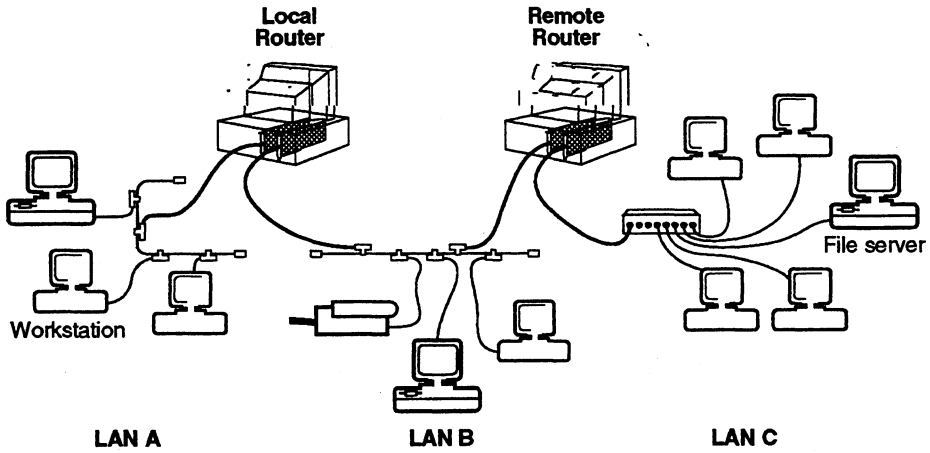
A workstation or file server running software that manages the exchange of information (in the form of data packets) between network cabling systems.

NetWare routers, unlike bridges, do more than transfer data packets between networks that use the same communications protocol. NetWare routers are intelligent. They not only pass packets of data between different cabling systems, but they also route the packets by way of the most efficient path.

An external router runs in a networked computer that is not a file server. It manages packet routing with its ROUTER.EXE file. The following figure illustrates an external router.



In the next example, if workstation requests on LAN A pass through a router connected to LAN A and then through a second router connecting LANs B and C, the router connecting LANs B and C is a remote router.



If the router connects to a modem, it is also a remote router.

Dedicated vs. Nondedicated External Routers

A dedicated router is a computer that works only as a router; it cannot function simultaneously as a workstation.

A dedicated router has greater reliability. Since no workstation applications run on this kind of router, they cannot hang the router. Router failure stops data sharing between networks, and brings down any workstations connected to the file server through the router.

A nondedicated router functions both as a router and as a workstation, eliminating the expense of buying another computer. In a nondedicated router, the workstation's NetWare shell runs on top of the router software. Therefore, deciding to use a dedicated or a nondedicated router involves the tradeoff between hardware cost and the risk of router failure.

Real Mode vs. Protected Mode

The type of microprocessor your router has and the amount of memory installed determine whether you should have ROUTER.EXE run in real or protected mode.

Router	8086, 8088, 80286, or 80386	80286 or 80386 with 1MB to 11MB additional memory
Dedicated Real Mode	X	
Nondedicated Protected Mode		X
Dedicated Protected Mode		X

NetWare protected mode routers that contain an 80286 or 80386 microprocessor can have up to 11MB of extended memory (though 4MB is usually an optimum amount). Memory above 1MB allows ROUTER.EXE and Value-Added Processes (VAPs) to run together on the router.

Programs that run in extended memory are in protected mode, protected against interference from other programs.

NetWare real mode routers that contain an 8086, 8088, 80286, or 80386 microprocessor and have the standard 640KB of base memory are called real-mode routers. The limited memory allows only one or two VAPs to run on the router.

See also **Bridge**.

Routing buffers

Portions of memory reserved in a router computer's RAM. Routing buffers are used to temporarily store and queue the message packets sent between communicating network stations when the network bus is busy.

Router Information Protocol (RIP)

A protocol used by routers to deliver routing information between routers.

When a router is initialized, it sends RIP packets that broadcast its location and request information about the network. From the returning RIP packets, the router creates a Router Information Table. The router uses the table to determine how far away each router is and the shortest route to each one.

RIP is based on distance-vector algorithms that measure the shortest path between two nodes on a network. It measures hops between each node.

SSS

SAP

See **Service Advertising Protocol.**

SCSI

(Small Computer System Interface) An industry standard that sets guidelines for connecting peripheral devices and their controllers to a microprocessor. The SCSI defines both hardware and software standards for communication between a host computer and a peripheral. Computers and peripheral devices that are designed to meet SCSI specifications are assured a large degree of compatibility.

Search drive

A drive that is searched by the operating system when a requested file is not found in the current (default) directory. The operating system checks search drives for executable files or data files accessed by the executable files. A search drive allows a user working in one directory to transparently access an application or data file that is located in another directory.

See also **Drive mapping.**

Security

NetWare provides an extensive security system that controls access to information stored on network volumes. Network security has three levels:

- Login security
- Rights security
- Attribute security

NetWare security controls

- Who can access the network;
- What resources (directories and files) users can access;
- What users can do with those resources (for example, read or modify a file);
- Who can perform tasks at the file server console.

This entry explains NetWare security, provides guidelines for planning security, and lists the utilities available for establishing and monitoring security.

Login Security

Login security controls access to the network. It determines which users can work on the file server, when they can work, what workstations they can work from, and which resources they can use. The network supervisor establishes login security by assigning usernames, requiring passwords, and setting up restrictions.

Usernames provide the first level of security. Only network supervisors and Workgroup Managers can create usernames. To access the file server, users must know a username (and its corresponding password if one is required). The usernames are kept in the file server's bindery and are assigned properties. As you assign properties to usernames, you grant the users sufficient security clearance to do their jobs.

All users are automatically assigned a password property and a membership-to-the-group-EVERYONE property.

Passwords are optional. However, if you don't require passwords, any person who knows a valid username can access the file server. A password's confidentiality is protected by NetWare. When you type a password at a workstation, the password is not displayed on the monitor. NetWare v3.*x* encrypts the password at the workstation and stores it on the hard disk in its encrypted form.

If you require passwords, you can either assign and change user passwords yourself or assign an initial password and allow the users to choose and change their own passwords.

If you allow users to change their own passwords, you can increase password security by requiring any or all of the following.

- A minimum password length. The default is at least five characters and prevents the use of passwords that are so short that they can be easily guessed. (The maximum length is 20 characters.)

- A periodic change in the password. The default is every 40 days and prevents users from keeping a password indefinitely.

- A unique password. The file server remembers the last 10 passwords that have been used for at least one day. This option prevents users from alternating between two favorite passwords. The one-day minimum prevents them from making ten changes in one day to return to a favorite password.

- A limited number of grace logins after a password has expired. (The default is six logins.) This option prevents users from unlimited use of an expired password.

Restrictions control when and where a user can log in and protect your network from intruders. You can use any of three types of login restrictions: station, time, and account.

- Station restrictions limit where a user can log in from. You can specify the workstations a user can log in from and the number of workstations a user can be logged in from concurrently.

- Time restrictions limit when users can log in. You can restrict users to specific days and hours.

- Account restrictions lock a user's account when certain limits are exceeded. When an account is locked, no one can log in to the file server using that username. You can have an account locked automatically when an account expires, when an account's balance is depleted, and when a set number of incorrect password uses is exceeded.

Related utility: **SYSCON** (*Utilities*).

Rights Security

Rights security controls which directories, subdirectories, and files a user can access and what the user is allowed to do with them. Rights security is controlled by trustee assignments and by the Inherited Rights Mask (IRM).

- Trustee assignments grant rights to specific users (or groups) that allow them to use a file or directory in particular ways (for example, only for reading). The network supervisor can select the appropriate rights to assign to users or groups in each directory or file.

  A trustee assignment grants users the right to see to the root of a directory. However, the users can't see any of the subdirectories unless they also have been granted rights in the subdirectories.

- Inherited Rights Masks are given to each file and directory when they are created. The default IRM includes all rights. But this does not mean that users have all rights; users can only use the rights that they have been granted in trustee assignments.

  If the IRM is modified for a file or subdirectory below the original trustee assignment, the only rights the user can inherit for the file or subdirectory are rights that are allowed by the IRM. For example, if a user is granted the Read right with a directory trustee assignment, the right to read files in a subdirectory could be revoked by having the Read right removed from the subdirectory's IRM.

Both trustee assignments and Inherited Rights Masks use the same eight trustee rights to control access to directories and files. Each right is represented by its initial.

S Supervisory
R Read
W Write
C Create
E Erase
M Modify
F File Scan
A Access Control

NetWare utilities display the initial letters of these rights between brackets as shown below.

```
[S R W C E M F A]
```

By convention, if some rights have either been revoked or have not been assigned, the absence of each is indicated by a blank space, as in the following.

```
[  R          F  ]
```

Although the same letter is used for both trustee assignments and IRMs, the meaning and effect depend on whether the right is assigned to a file or a directory. Each right is defined twice below, once in "Directory Rights" and again in "File Rights."

Directory rights control general access to the directory, its files, and subdirectories. When granted at the directory level, the rights apply to all the files and subdirectories in that directory unless redefined at the file or subdirectory level.

When assigned to a directory, the rights have the following effects.

- Supervisory. Grants all rights to the directory, its files, and its subdirectories. The Supervisory right overrides any restrictions placed on subdirectories or files with an Inherited Rights Mask. Users who have this right in a directory can grant other users Supervisory rights to the directory, its files, and its subdirectories. Once the Supervisory right has been granted, it can be revoked only from the directory to which it was granted. It cannot be revoked in a file or subdirectory.

- Read. Grants the right to open files in a directory and read their contents or run the programs.

- Write. Grants the right to open and modify files.

- Create. Grants the right to create files and subdirectories in the directory. If Create is the only right granted at the directory level and no rights below the directory are granted, this right creates a drop box directory.

In a drop box directory, users can create a file, and then open and write to it. Once the file is closed, however, they cannot see or modify the file. They can also copy files or subdirectories into the directory. When they copy, they assume ownership of the files and subdirectories. However, any trustee assignments assigned to the files or subdirectories are revoked.

- Erase. Grants the right to delete a directory, its files, its subdirectories, and its subdirectory files.

- Modify. Grants the right to change directory and file attributes. Also grants the right to rename the directory, its files, and its subdirectories. This right does not grant the right to modify the contents of a file.

- File Scan. Grants the right to see directory files.

- Access Control. Grants the right to modify a directory's or a file's trustee assignments and Inherited Rights Mask (IRM). Users can also modify file trustee assignments and IRMs. Users can grant any right (except Supervisor) to any other user, including rights that the themselves have not been granted.

Related utilities: To grant or modify a directory trustee assignment, use **FILER; GRANT; REMOVE; REVOKE; SYSCON** (*Utilities*).

Related utilities: To modify a directory's IRM, use **ALLOW; FILER** (*Utilities*).

File rights control access to specific files in a directory. They are used to redefine the rights that users inherit from directory rights. The following rights control access to specific files.

- Supervisor. Grants all rights to the file. Users who have this right can grant any right to another user and can modify all rights in the file's IRM.

- Read. Grants the right to open and read the file.

- Create. It can be set, but it has no effect.

- Write. Grants the right to open and write to the file.

- **Erase.** Grants the right to delete the file.

- **Modify.** Grants the right to change the file's attributes and rename the file, but not the right to modify the contents of the file.

- File Scan. Grants the right to see the filename when viewing the directory. Grants the right to see the directory structure, from the file to the root of the directory.

- Access Control. Grants the right to modify the file's trustee assignments and Inherited Rights Mask. Users who have this right can grant all file rights, except Supervisor, to other users, including rights that they themselves have not been granted.

Related utilities: To grant or modify file trustee assignments, use **FILER; GRANT; REMOVE; REVOKE; SYSCON** (*Utilities*).

Related utilities: To modify the file's IRM, use **ALLOW; FILER** (*Utilities*).

Effective Rights

Effective rights are the rights a user can actually exercise in a given directory or file. To determine a user's effective rights, you must know

- What rights were granted in the trustee assignments for the user;

- What rights were granted in the trustee assignments for the groups the user belongs to;

- What rights were revoked with the Inherited Rights Masks.

Related Utilities: To view effective rights, use **FILER; RIGHTS; WHOAMI** (*Utilities*).

The following examples explain how effective rights are determined for a directory and a file. In the diagrams, Inherited Rights Mask is abbreviated to IRM and trustee assignment is abbreviated TA.

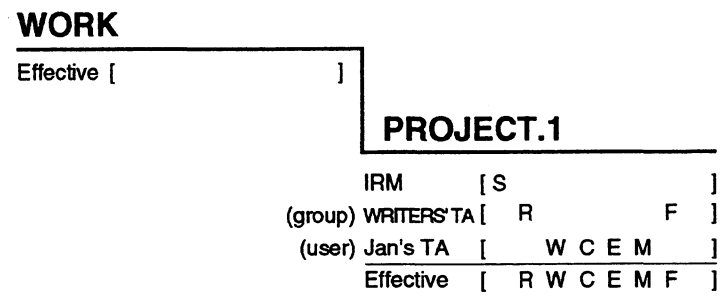
Directory effective rights. In directories, effective rights are determined by one of two methods:

- By calculating the effective rights in the parent directory (including the Supervisor right) and then determining which rights the directory's Inherited Rights Mask will allow to filter through;

- By granting a user a trustee assignment to a directory.

In a directory, trustee assignments override the directory's Inherited Rights Mask. If trustee assignments are granted, a user's effective rights are determined solely by the trustee assignments (user plus group trustee assignments).

The following diagram is an example of determining the effective rights for Jan in the directory WORK\PROJECT.1.



Since Jan's user trustee assignment was W, C, E, and M and the group WRITERS was assigned R and F, the sum of these trustee assignments are her effective rights in the PROJECT.1 directory.

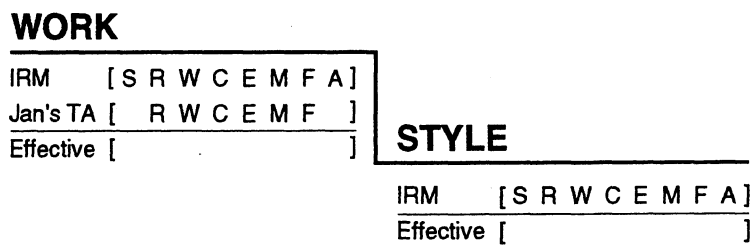
Since she was granted a trustee assignment to PROJECT.1, Jan has limited File Scan rights in WORK. She can see PROJECT.1 when scanning the WORK directory.

In the examples on the following pages, Example 1 explains how to determine rights if no new trustee assignments are granted the user. Example 2 explains how to determine rights when a new trustee assignment is granted to the user. Example 3 explains how to determine rights when the Supervisor right has been granted.

Example 1

If no new trustee assignments are granted, the Inherited Rights Mask determines which effective rights a user can inherit from the parent directory.

Step 1: To calculate the rights, first determine a user's effective rights in the parent directory. In the following example, calculate Jan's effective rights for the WORK directory.

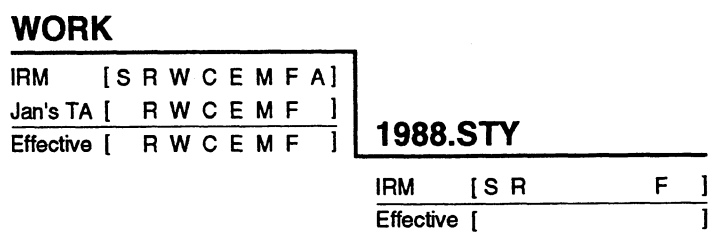


In this example, Jan's effective rights in the WORK directory are R, W, C, E, M, and F.

Step 2: View the Inherited Rights Mask of the STYLE directory.

- If the mask has all rights, the user's effective rights in the STYLE directory are the effective rights of the WORK directory.
- If the STYLE directory's Inherited Rights Mask is modified by revoking some of the rights, the parent effective rights must be matched with the remaining rights in the mask. Only those that match will be effective rights in the STYLE directory.

In the previous example, Jan's effective rights in the STYLE directory are R, W, C, E, M, and F because the mask allows all rights to be inherited. What are they in the following example?

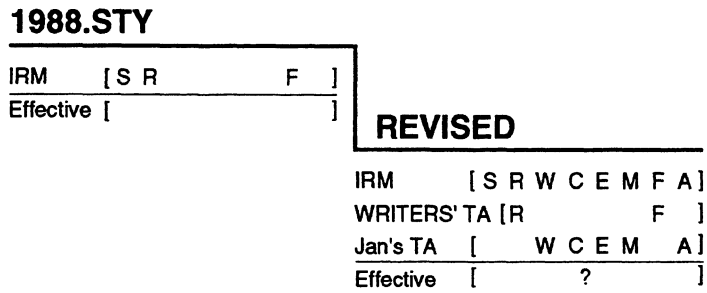


In the previous example, Jan's effective rights in the 1988.ST directory are R and F. Supervisor right has not been revoked from the Inherited Rights Mask. This right cannot be revoked from an Inherited Rights Mask. However, as this example shows, the S right in the mask has no effect if it hasn't been granted to the user.

Example 2

If a trustee assignment is made to a directory, the trustee assignment overrides the effective rights from the parent directory and the current directory's Inherited Rights Mask. The user's effective rights are those granted in the trustee assignment.

For example, Jan's effective rights in the 1988.ST directory are R and F. What are Jan's effective rights in the REVISED directory?

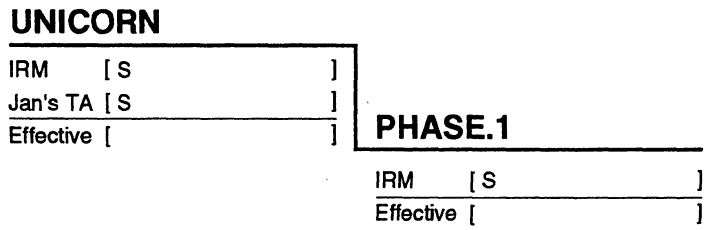


Jan's effective rights in the REVISED directory are R, W, C, E, M, F, and A.

Example 3

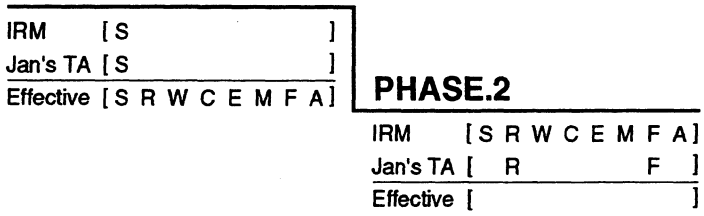
If a user has been granted the Supervisor right in the parent directory, the user has all rights to all directories below it regardless of trustee assignments or modification of Inherited Rights Masks.

For example, suppose Jan is the supervisor of a new project with the code name "Unicorn." Since Jan is the project supervisor, the network supervisor grants her the Supervisor right to the UNICORN directory containing the project. What are Jan's effective rights in the UNICORN directory? What are her rights in the PHASE.1 directory?



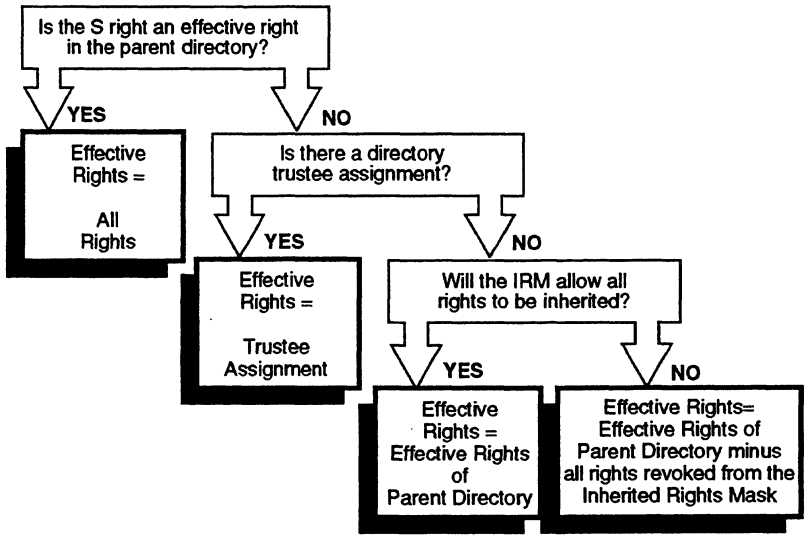
Jan's effective rights in the UNICORN directory are all rights: S, R, W, C, E, M, F, and A. She has the same rights in the PHASE.1 directory.

In the next example, Jan's rights were redefined in the PHASE.2 directory with a new trustee assignment. What are Jan's effective rights in the PHASE.2 directory?



Jan's effective rights in the PHASE.2 directory are still all rights. Her rights cannot be redefined below the UNICORN directory because she was granted the Supervisor right to the UNICORN directory.

Summary for determining directory effective rights. The following figure summarizes the principles governing effective rights in directories.



File effective rights are determined in nearly the same way as subdirectory effective rights:

- By calculating the effective rights in the directory and then determining which rights the file's Inherited Rights Mask will allow to filter through;
- By granting a user a trustee assignment to the file;
- By determining the user's effective rights (including the Supervisor right) in the parent directory.

In the examples on the following pages, Example 1 explains how to determine rights if no new trustee assignments are granted at the file level. Example 2 explains how to determine rights when a new trustee assignment is granted at the file level. Example 3 explains how to determine rights when the Supervisor right has been granted.

NOTE

If you are using an application that creates extra files (such as backup files), you need to assign the user the Create right in the directory that the application places those files.

Example 1

If no new trustee assignments are granted for the file, the file's Inherited Rights Mask determines which effective rights a user can inherit from the directory.

Step 1: To calculate the rights, first determine a user's effective rights in the parent directory. In the following example, calculate Jan's effective rights for the WORK directory.

WORK

IRM	[S R W C E M F A]
Jan's TA	[R W C E M F]
Effective	[ ]

FILE.1

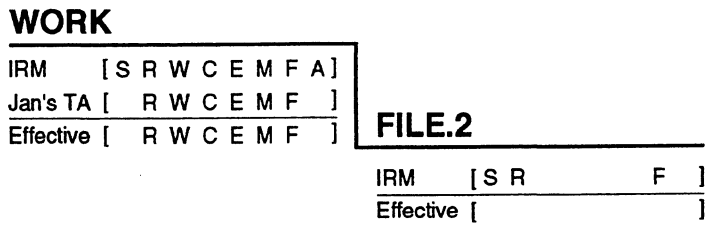
IRM	[S R W C E M F A]
Effective	[ ]

In this example, Jan's effective rights in the WORK directory are R, W, C, E, M, and F.

Step 2: View the Inherited Rights Mask of the file.

- If the mask has all rights, the user's effective rights in the file are the effective rights of the parent directory.
- If the file's Inherited Rights Mask is modified by revoking some of the rights, the directory effective rights must be matched with the remaining rights in the mask. Only those that match will be an effective right in the file.

In the previous example, Jan's effective rights to the FILE.1 file are R, W, C, E, M, and F because the mask allows all rights to be inherited. What are they in the following example?

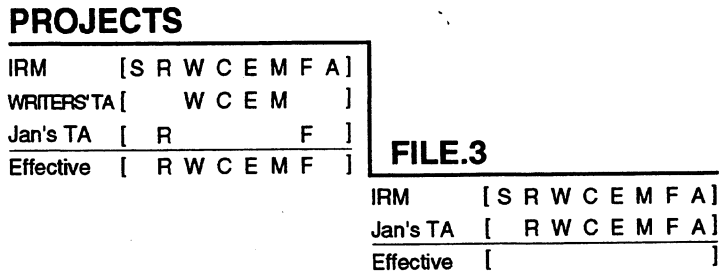


In this example, Jan's effective rights in FILE.2 are R and F. Notice that the Supervisor right has not been revoked from the Inherited Rights Mask. This right cannot be revoked from an IRM. However, as this example shows, the S right in the mask has no effect if it hasn't been granted to the user.

Example 2

If a trustee assignment is granted to a file, effective rights are determined the same as directory rights. The trustee assignment overrides the effective rights from the parent directory and the file's Inherited Rights Mask. The user's effective rights are those granted in the user and group trustee assignments.

For example, Jan's effective rights in the PROJECTS directory are R, W, C, E, M and F. What are Jan's effective rights to the FILE.3 file?

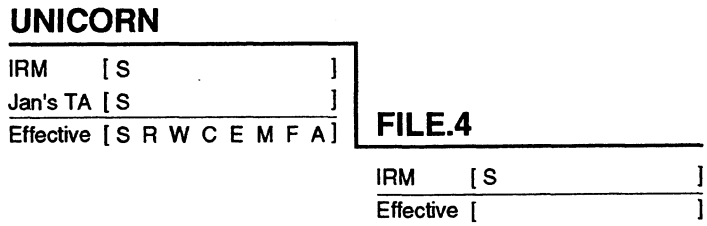


Jan's effective rights to FILE.3 are R, W, C, E, M, F, and A.

Example 3

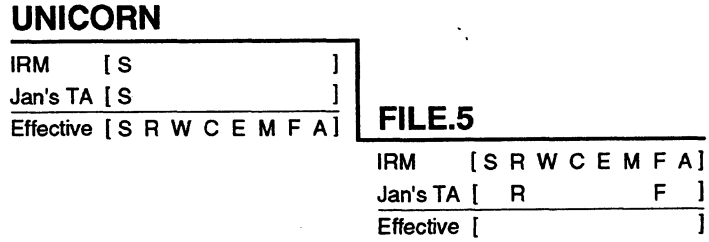
If a user has been granted the Supervisor right in the parent directory, the user has all rights to the files regardless of other trustee assignments or modification of Inherited Rights Masks.

In the following example, Jan was made supervisor of a new project with the code name "Unicorn." Since Jan is the project supervisor, the network SUPERVISOR grants her the Supervisor right to directory UNICORN containing the project. What are her rights to FILE.4?



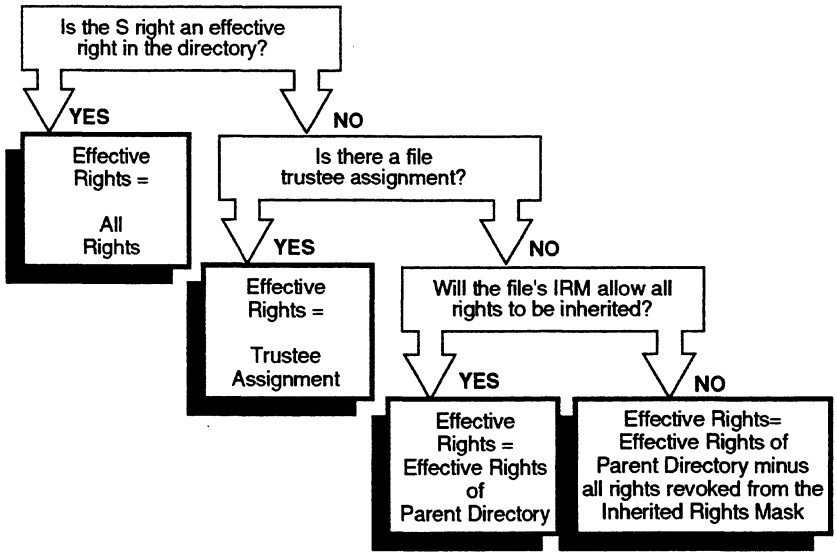
Jan's effective rights to FILE.4 are all rights.

In the following example, Jan's rights were redefined in the FILE.5 file with a new trustee assignment. What are Jan's effective rights in the FILE.5 file?



Jan's effective rights in the FILE.5 file are still all rights. Her rights cannot be redefined below the UNICORN directory because she was granted the Supervisor right to the UNICORN directory.

Summary for Determining File Effective Rights. The following figure summarizes the principles governing effective rights for files.



Assigning Rights

You can grant a combination of rights, although some combinations are not useful. See the following examples.

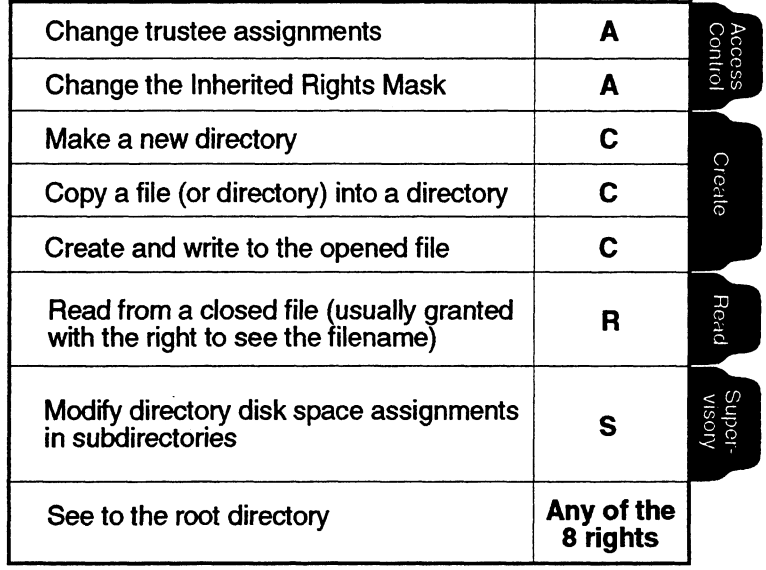
- You could grant a user only the Supervisor right to a directory and revoke all other rights. However, that user would still have all rights to the directory.

- You could grant a user only Read and File Scan rights, without knowing that the application which this user needs to run creates temporary files when accessed. This user will not be able to work because the Create, Erase, and Modify rights have not been granted.

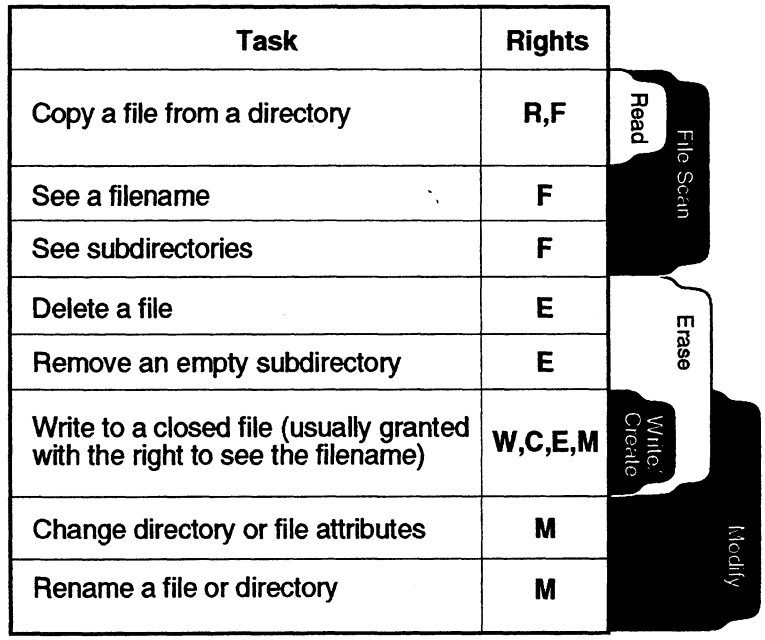
Rights need to be granted carefully. If you grant users more than they need, they can delete, corrupt, or steal data. If you grant them too few, they will not be able to do the work assigned to them.

Users need to be assigned the following rights to perform the indicated tasks.

Task	Rights
Change trustee assignments	A
Change the Inherited Rights Mask	A
Make a new directory	C
Copy a file (or directory) into a directory	C
Create and write to the opened file	C
Read from a closed file (usually granted with the right to see the filename)	R
Modify directory disk space assignments in subdirectories	S
See to the root directory	Any of the 8 rights



Task	Rights
Copy a file from a directory	R,F
See a filename	F
See subdirectories	F
Delete a file	E
Remove an empty subdirectory	E
Write to a closed file (usually granted with the right to see the filename)	W,C,E,M
Change directory or file attributes	M
Rename a file or directory	M



When assigning rights to application directories, check the application documentation. If possible, separate the files that users create when they use the application from the executable files needed to run the application. Normally users only need R and F rights to directories with executable files while they need R, F, C, E, and M rights to directories in which they create files. If the applications are put in a search directory, the users can access the applications from another directory in which they have the additional rights they need to create files.

Sample Scenario

The scenario described below clarifies the interaction between trustee assignments and Inherited Rights Masks and demonstrates one method of assigning rights.

Suppose that the following groups and supervisors have been created.

Project Supervisors	Group
Mel	Macintosh Writers
Pam	PC Writers
Jan	Editing

Suppose that the following users have been assigned to the groups.

Macintosh Writers	PC Writers	Editors
Group name: MAC	Group name: PC	Group name: EDITORS
Group Members	Group Members	Group Members
Mel (supervisor)	Pam (supervisor)	Jan (supervisor)
Mike	Pat	Janene
Mary	Paul	Jean
Mona	Peter	Judy

In the following diagram, these users and groups have been granted trustee assignments to various directories in the SYS volume. The rights allowed by the Inherited Rights Mask (IRM) are listed right under the directory's name. For example,

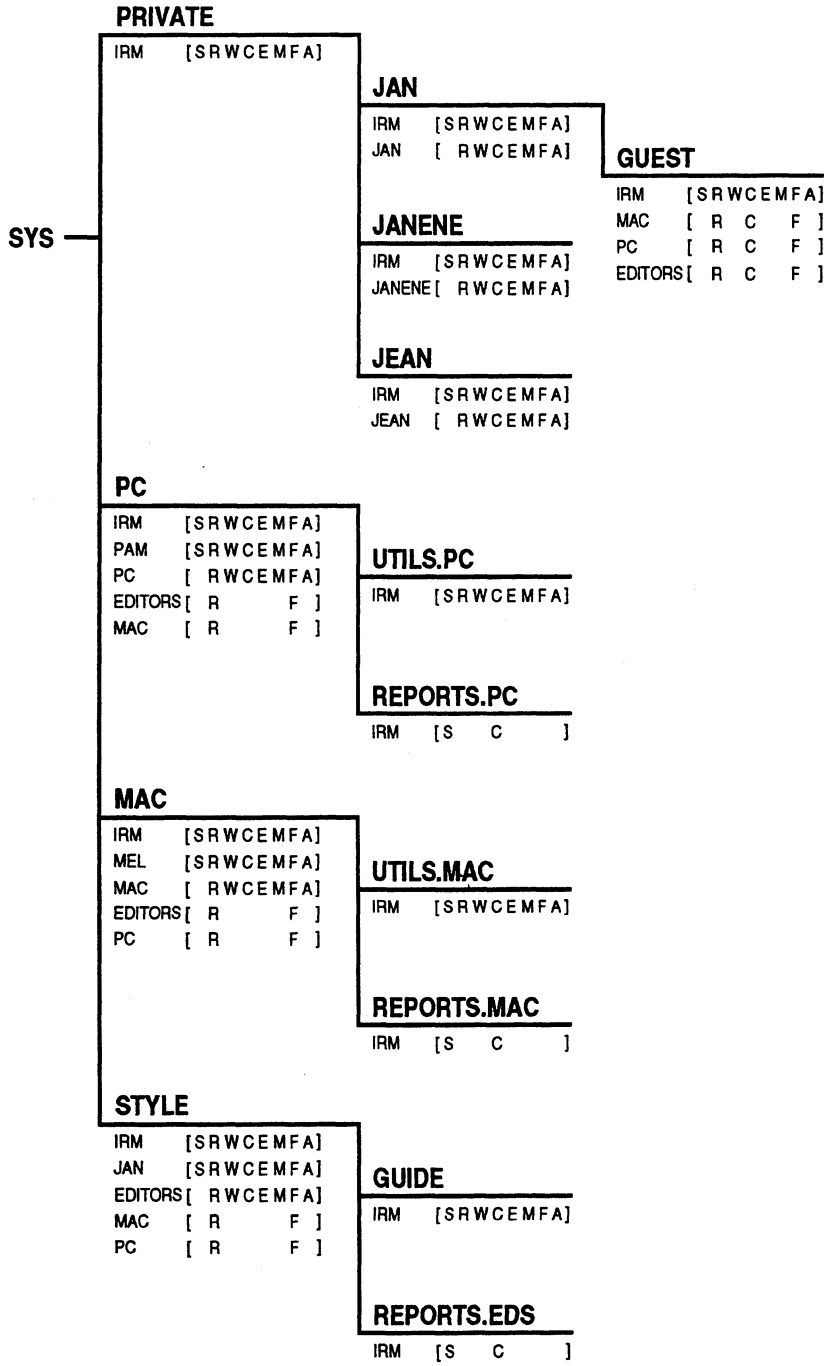
```
IRM  [S  C     ]
```

indicates that the IRM has been modified to allow only the Supervisory and Create right to be inherited. The trustee assignments are listed below the IRM and are preceded by either the group's or user's name. For example,

```
[SRWCEMFA]
```

would be Pam's trustee assignment for the directory.

The pages following the diagram pose some questions, asking you to determine the effective rights of users in some of the directories and the tasks that they can perform in certain directories. Following the questions, the correct answers are given with explanations.



Questions. Answer the following questions. The answers to the questions follow.

1. What effective rights can the supervisor of the editing group, JAN, exercise in the following directories? Circle the rights that have been granted to JAN as a user or through her membership to the group EDITORS.

SYS:PRIVATE/JEAN	S R W C E M F A
SYS:STYLE/REPORTS.EDS	S R W C E M F A
SYS:PC/REPORTS.PC	S R W C E M F A
SYS:MAC/UTILS.MAC	S R W C E M F A

2. What effective rights can PETER exercise in the following directories? Circle the rights that have been granted to PETER as a user or through his membership to the group PC.

SYS:PRIVATE/JAN/GUEST	S R W C E M F A
SYS:PC/REPORTS.PC	S R W C E M F A
SYS:PC/UTILS.PC	S R W C E M F A

3. Can MARY, who is a member of the group MAC, copy a file from any of the directories listed below? Circle the correct answers.

SYS:PC/UTILS.PC	Yes	No
SYS:MAC/REPORTS.MAC	Yes	No

4. Can MEL, who is the supervisor and a member of the group MAC, see and read files in any of the directories listed below? Circle the correct answers.

SYS:MAC/REPORTS.MAC	Yes	No
SYS:STYLE/GUIDE	Yes	No

5. Can JEAN, who is a member of the group EDITORS, create or copy a file into any of the directories listed below? Circle the correct answers.

SYS:STYLE/REPORTS.EDS	Yes	No
SYS:PRIVATE/JEAN	Yes	No
SYS:PRIVATE/JAN/GUEST	Yes	No

Answers. The answers to the questions appear below with a brief explanation.

1. What effective rights can the supervisor of the editing group, JAN, exercise in the following directories? Circle the rights that have been granted to Jan as a user or through her membership to the group EDITORS.

   SYS:PRIVATE/JEAN: None. JAN cannot even see the directory because she has not been granted any rights to the directory.

   SYS:STYLE/REPORTS.EDS: All rights: [S R W C E M F A]. Since JAN was granted the Supervisory right to the STYLE directory, she has all rights in all of its subdirectories regardless of how the IRM is set.

   SYS:PC/REPORTS.PC: None. All of JAN's rights (RF) are revoked with the IRM of the directory; therefore, JAN cannot even see this directory.

   SYS:MAC/UTILS.MAC: R and F. These are the only rights JAN was granted through her membership in the EDITORS group.

2. What effective rights can PETER exercise in the following directories? Circle the rights that have been granted to PETER as a user or through his membership to the group PC.

   SYS:PRIVATE/JAN/GUEST: R, C, and F. PETER is a member of the PC group, and the PC group was granted RCF rights to the directory. If JAN wants all users on the file server to have R, C and F, a more effective method is to grant the R, C, and F rights to group EVERYONE. Since JAN has the A right, she can make this assignment using FILER or GRANT.

SYS:PC/REPORTS.PC: C. All other rights granted to PAM in the PC directory (through membership in the PC group) have been revoked in the IRM of the REPORTS.PC directory

SYS:PC/UTILS.PC: R W C E M F. The PC group was granted these rights in the PC directory, PAM is a member of the PC group, and the IRM allows all of these rights to be inherited.

3. Can MARY, who is a member of the group MAC, copy a file from any of the directories listed below? Circle the correct answer.

   SYS:PC/UTILS.PC: Yes. MARY is a member of the MAC group, and MAC has been granted RF rights to the directory.

   SYS:MAC/REPORTS.MAC: No. Even though MARY was granted the RF rights in the MAC directory, those rights are revoked in the IRM of the REPORTS.MAC directory.

4. Can MEL, who is the supervisor and a member of group MAC, see and read files in any of the directories listed below? Circle the correct answer.

   SYS:MAC/REPORTS.MAC: Yes. Even though the IRM revokes the RF rights, MEL has been granted the Supervisory right to the MAC directory and, therefore, can exercise all rights in all of MAC's subdirectories.

   SYS:STYLE/GUIDE: Yes. The IRM does not revoke the RF rights, MEL is a member of the MAC group, and the MAC group was granted RF rights to the STYLE directory.

5. Can JEAN, who is a member of group EDITORS, create or copy a file into any of the directories listed below? Circle the correct answer.

   SYS:STYLE/REPORTS.EDS: Yes. The IRM does not revoke the Create right, JEAN is a member of the EDITORS group, and the EDITORS group was granted the Create right in the STYLE directory.

   SYS:PRIVATE/JEAN: Yes. This directory is JEAN's private directory, and she has been granted all rights except Supervisory to the directory.

SYS:PRIVATE/JAN/GUEST: Yes. The EDITORS group was granted the Create right to the directory, and JEAN is a member of the EDITORS group.

Attribute Security

Attribute security assigns special properties to individual directories or files. Attribute security overrides rights granted with trustee assignments and can prevent tasks that effective rights would allow. For example, attributes can be used to prevent the following.

- Deleting a file or a directory
- Copying a file
- Viewing a file or a directory
- Writing to a file

Attributes are also used for the following.

- Controlling whether files can be shared so that only one or many can access the file at the same time
- Marking files as modified so that backup utilities can select only the files that have been modified
- Protecting files from data corruption by ensuring that either all changes are made or no changes are made when a file is being modified.

If users have the Modify right for the directory or the file, they can change the attributes and complete any task allowed with their effective rights.

NetWare uses the following attributes (represented by the indicated letters). The following chart lists directory and file attributes:

Attributes	Letter	Directory	File	Description
Archive needed	A		✓	Identifies files modified after last backup. Assigned automatically.
Copy Inhibit	C		✓	Prevents Macintosh users from copying a file. Overrides Read and File Scan rights. Modify right required to remove this attribute.
Delete Inhibit	D	✓	✓	Prevents users from erasing directories or files. Overrides Erase right. Modify right required to remove this attribute.
Execute Only	X		✓	Prevents copying or backing up files. Attribute cannot be removed. Assign only to files with an .EXE or .COM extension (program files). Keep a duplicate copy of these files in case they become corrupted and need to be replaced. CAUTION: Some programs will not execute properly if flagged Execute Only.
Hidden	H	✓	✓	Hides directories and files from DOS DIR scans and prevents them from being deleted or copied. Directories and files appear in NetWare NDIR scans if a user has the File Scan right.
Indexed	I		✓	Not currently used by NetWare. Can be set, but has no effect.
Purge	P	✓	✓	Purges a file as soon as it is deleted if the file is flagged with this attribute or resides in a directory flagged with this attribute.
Read Audit	Ra		✓	Not currently used by NetWare. Can be set, but has no effect.
Read Only/ Read Write	Ro/Rw		✓	Indicates whether a file can be modified. All files are flagged Read Write when they are created and can be modified unless the Read Only attribute is set. Assigning Ro activates Delete Inhibit and Rename Inhibit. Modify right required to remove the Ro attribute.
Rename Inhibit	R	✓	✓	Prevents users from renaming directories or files. Modify right required to remove this attribute.
Shareable	S		✓	Allows several users to access a file simultaneously. Usually used in combination with the Read Only attribute.
System	Sy	✓	✓	Assign to system files and their directories. Hides these directories and files from DOS DIR scans and prevents them from being deleted or copied. Directories and files appear in NetWare NDIR scans if a user has the File Scan right.
Transactional	T		✓	Not currently used by NetWare. Can be set, but has no effect.
Write Audit	Wa		✓	Not currently used by NetWare. Can be set, but has no effect.

The initial letters of these attributes are displayed between brackets by NetWare utilities.

```
[Ro S A X H Sy I T P Ra Wa C D R]
```

By convention, attributes that have not been assigned are indicated by blank space, as in the following.

```
[Ro S                          D R]
```

Use directory and file attributes to increase security in areas where many users have access to files. For example, NetWare utilities are flagged so that even SUPERVISOR cannot accidentally delete them without removing flags.

- All NetWare files in SYS:SYSTEM, SYS:PUBLIC, and SYS:LOGIN are automatically flagged Ro, S, D, and R.

- The bindery files are automatically flagged Sy, H, and T.

Related utilities: To change or display file attributes, see **FILER**; **FLAG** (*Utilities*).

Related utilities: To change or display directory attributes, see **FILER**; **FLAGDIR** (*Utilities*).

Related utilities: **ALLOW**; **FILER**; **FLAG**; **FLAGDIR**; **GRANT**; **REMOVE**; **REVOKE**; **RIGHTS**; **SYSCON**; **WHOAMI** (*Utilities*).

Security equivalence

The ability to give one user the same rights as another. Use security equivalence when you need to give a user temporary access to the same information or rights another user has access to. By using a security equivalence, you avoid having to review the whole directory structure and determine which rights need to be assigned in which directories or to which files.

SUPERVISOR can make any user security equivalent to another user or group, but Workgroup Managers and User Account Managers can assign security equivalences only within the pool of users and groups they manage. In networks containing confidential data that only selected users have access to, take care that you do not inadvertently give a user access to restricted information. Also, be aware that during the period the security equivalence is in effect, a user who is security equivalent to another user has all rights to that other user's home directory. Making a user security equivalent to a group would not have that disadvantage.

Be particularly cautious in making any user security equivalent to SUPERVISOR. Instead, delegate responsibilities to managers and operators.

See also **User; User Account Manager; Workgroup Manager.**

Related utility: **SYSCON** (*Utilities*).

Semaphores

Part of the operating system that coordinates activities of both programs and processes to prevent data corruption in multi-process environments. One use of semaphores is to provide a system of file sharing and file locking.

See also **File locking.**

Serial communication

A data channel that sends information one bit at a time. NetWare uses the RS-232 serial communications standard to send information to serial printers, remote workstations, remote routers, and asynchronous communication servers. This standard, developed by the Electronic Industries Association (EIA), is used to aid in the delivery of information from one system to another. A system can be any device or group of devices that can handle and process the data it receives. For example, a printer can be thought of as a system that transforms the binary data it receives from the computer to printed text. The RS-232 standard uses several parameters that must match on both systems for valid information to be transferred. These parameters include baud rate, character length, parity, stop bit, and XON/XOFF.

Baud Rate is the signal modulation rate, or the speed at which a signal changes. Since most modems or serial printers attached to personal computers send only one bit per signaling event, baud can be thought of as bits per second; however, higher-speed modems may transfer several bits per signal change. Typical baud rates are 300, 1200, 4800, and 9600. The higher the number, the greater number of signal changes and, therefore, the faster the transmission.

Character length specifies the number of bits used to form a character. The standard ASCII character set (including letters, numerals, and punctuation) consists of 128 characters; this requires a character length of 7 bits for transmissions ($2^7 = 128$). Extended character sets contain an additional 128 characters, such as the line drawing or foreign-language characters used in IBM's extended character set. For a transmission to include characters from an extended character set, the character length must be 8 ($2^8 = 256$).

Parity is the method of checking for errors in transmitted data. Parity can be set to odd or even, or not used at all. When the character length is 8, parity checking is not used (because there are no spare bits in the byte). When the character length is 7, the eighth bit in each byte is randomly set to 0 or 1 such that the sum of bits (0s and 1s) in the byte is either odd or even (depending on the parity setting). For example:

7-bit charater	With Parity bit (odd parity)	With Parity bit (even parity)
1000001 (A)	10000011	10000010
1000010 (C)	10000110	10000111
1011000 (X)	10110000	10110001
1011010 (Z)	10110101	10110100

When each character is received, its parity is checked again. If the parity is incorrect (because the bit was changed during transmission), the communications software determines that an error has occurred during transmission and can request that the data be retransmitted.

Stop bit is a special signal that indicates the end of a character. Today's modems are fast enough that the stop bit is always set to one. Slower modems used to require two stop bits.

XON/XOFF is one of many methods used to prevent the sending system from transmitting data faster than the receiving system can accept the information.

Serial port

A port that allows data to be transmitted asynchronously, one bit at a time. On IBM PC-compatible computers, COM1 and COM2 are asynchronous serial ports.

Serialization

The means NetWare uses to identify a unique copy of the operating system. If two NetWare operating systems with the same serial number co-exist on the same internetwork, each file server displays a copyright violation warning at the file server console and at each logged-in workstation.

Server

See **File server; Print server.**

Server protocol

See **NCP service protocol.**

Service Advertising Protocol (SAP)

A protocol used to report the existence of services on the network. When a file server comes up, it uses the SAP daemon to send the following information to the network:

- File server name
- File server address
- Available services

File servers, print servers, NVT servers, and communications servers advertise using SAP every sixty seconds.

From the information received about other entities using SAP, the file server creates a Service Information Table. From information in the Service Information Table, the file server determines how far away each service is and the shortest route to each service.

Service engine

A process initialized by the NetWare daemon. The service engine receives and processes NCP requests. It acts as the interface to the DG/UX file system to process the NCPs and formulate response NCPs.

The service engine also services AFP requests from Macintosh clients through a NetWare for Macintosh gateway.

Service engines synchronize through lock managers in shared memory.

Service protocol

See **NCP service protocol.**

Shareable attribute

See **Attributes; Security (Attribute Security).**

Shared memory

A pool of memory that different host processes have access to. Shared memory is synchronized and accessed through the use of semaphores. If a semaphore is in use, then that part of shared memory is locked to other processes. NetWare stores the following structures in shared memory:

- Connection tables
- Lock managers
- Bindery
- File server information
- Statistics
- Volume table

Shell

See **NetWare shell.**

SHELL.CFG file

A specialized text file created with any ASCII text editor and included on a workstation boot diskette with any other necessary boot files. Similar to the DOS CONFIG.SYS file, the SHELL.CFG file contains configuration values that are read and interpreted when your workstation starts up. These values adjust the operating parameters of the NetWare shell, IPX, or NetBIOS.

Because the NetWare shell is responsible for many routines and processes in a workstation, change the values of certain shell parameters to modify the shell's reaction to those routines and processes.

Applications such as database, multitasking, or NetBIOS (involved in peer-to-peer communications or distributed processing) may require parameter values different from the default values to properly function on the network. To find out which parameters to modify, consult the setup reference for each application used on

your network. Printing, file retrieval, and other network problems can be solved by adjusting shell parameters.

If you plan to use the DOS ODI shell, you can either incorporate the SHELL.CFG parameters into the NET.CFG file or use both files separately.

See also **BNETX.COM, Boot files; Communication protocols; EMSNETX.EXE; IPX; NetWare DOS shell; NETX.COM; XMSNETX.EXE.**

Small Computer Systems Interface

See **SCSI.**

Software interrupt

See **Interrupt.**

Source routing

IBM's method of routing data across routers. NetWare source routing programs allow an IBM Token-Ring Network Router to forward NetWare packets (or frames).

Single-route broadcasting means that only one designated single-route router will pass the packet and only one copy of the packet will arrive at its destination. Single-route broadcast routers can transmit both single-route and all-routes packets.

All-routes broadcasting sends the packet across every possible route in the network, resulting in as many copies of the frame at the destination as there are all-routes broadcasting routers in the network. All-routes broadcast routers only pass all-routes broadcast packets.

IBM routers can be configured as either single-route broadcast or all-routes broadcast. The default is single-route broadcast.

To support IBM hardware and applications, Novell provides the ROUTE.COM driver for workstations on the network. This driver allows users running NetWare to communicate across IBM Token-Ring Network Routers. It also allows IBM applications that require source routing support to run unmodified on NetWare.

At the workstation, the ROUTE.COM file determines the type of packets the workstation broadcasts. It should execute after IPXODI.COM and before the NetWare shell (such as NETX.COM). See the *NetWare for DOS* manuals.

Spool

A means of transferring data that was intended for a peripheral device (such as a printer) into temporary storage. From there the data can be transferred to the peripheral at a later time, without affecting or delaying the operating system as it performs other operations. In NetWare, the CAPTURE command is used to spool data.

SPX

(Sequenced Packet eXchange) A Novell communication protocol that monitors network transmissions to ensure successful delivery. SPX is derived from Novell's Internetwork Packet Exchange (IPX) using the Xerox Sequenced Packet Protocol. SPX enhances the IPX protocol by requesting a connection between the two end nodes first, before any data exchange takes place.

SPX tracks transmissions as a series of separate packets. SPX ensures that the data packet made it to the destination.

SPX is a connection-oriented protocol. Once a connection is established with a partner workstation or file server, SPX requests acknowledgements from and returns acknowledgements to the partner, ensuring successful data delivery. If an acknowledgement request brings no response within a specified time, SPX retransmits. After a reasonable number of retransmissions fail to return a positive acknowledgement, SPX assumes the connection has failed and warns the operator of the failure. SPX requires that each packet sent receives an acknowledgement from the partner before another packet is transmitted.

See also **Communication protocols; IPX; NetWare DOS shell.**

Station

See **Network station; Router; Workstation.**

Station address

See **Network number.**

Stop bit

See **Serial communication.**

STREAMS

A protocol service that provides a common interface between NetWare and transport protocols (such as IPX/SPX, TCP/IP, SNA, and OSI) that need to deliver data and requests to NetWare for processing.

Subdirectory

A directory below another in the directory structure. For example, in SYS:ACCTS/RECEIVE, RECEIVE is a subdirectory of SYS:ACCTS.

See also **Directory structure**.

SUPERVISOR

The username for the network supervisor or system administrator present in the bindery as a bindery object when the file server is first brought up. SUPERVISOR is assigned ID Number 1 and cannot be deleted or renamed. SUPERVISOR has all rights in all directories; these rights cannot be revoked. SUPERVISOR initially has no corresponding password so that the network supervisor can log in when setting up the network environment.

Delegating responsibility. As necessary, the network supervisor can delegate system administration responsibilities to Management Information System (MIS) staff or organization managers. Once the persons selected have been created as users on the file server, they can be designated as one of the following.

- **Workgroup Manager.** An assistant supervisor with rights to create bindery objects (such as users and groups) and manage the user accounts. A Workgroup Manager (or any other user) can also be designated as a User Account Manager for existing users.

- **User Account Manager.** A user with rights to manage user accounts, but no rights to create new bindery objects, such as users and groups. Workgroup Managers are User Account Managers for users they create. Existing users can be assigned to a Workgroup Manager (or any other user) for account management.

- **File server console operator.** A file server supervisor with rights to use the FCONSOLE utility.

- **Print server operator.** A print server supervisor with rights to manage the print server.

- **Print queue operator.** A printing supervisor with rights to create, manage, disable, and enable print queues.

Security. Because SUPERVISOR has absolute authority over users and information, use caution in making anyone security equivalent to SUPERVISOR. Instead, delegate supervisor responsibilities by designating operators and managers.

For maximum security, consider the following.

- Set a supervisor password in SYSCON the first time you log in as SUPERVISOR. Change this password regularly and do not select an obvious password, such as a spouse's name.

- Create a second username to use when you work on the network as a regular user. Log in as SUPERVISOR only when you perform SUPERVISOR tasks.

- Set up a "back door" to the system in one of two ways:

  1. Create a fictitious user with an unpredictable (but unforgettable) username and make that user security equivalent to SUPERVISOR.

  2. Create a fictitious user with an unpredictable (but unforgettable) username and make that user the User Account Manager for both the fictitious user and SUPERVISOR.

- Use caution in making anyone security equivalent to SUPERVISOR. Instead, delegate supervisor jobs by designating operators and managers.

See also **File server console operator; Print server operator; User; User Account Manager; Workgroup Manager.**

Related utility: **SYSCON** (*Utilities*).

Supervisory right

See **Rights; Security (Rights Security).**

Surge protectors/suppressors

See **Power conditioning.**

Switch block

A set of switches mounted together to form a single component. In some file servers, a switch block is used to control system configuration data, such as type of monitor, amount of memory, and number of drives. Network boards often use switch blocks to set system addresses (such as station, base I/O, and base memory addresses).

Synchronous transmission

See **Serial communication.**

System attribute

See **Attributes; Security (Attribute Security).**

SYSTEM directory

A directory created on volume SYS during network installation. Copy the NetWare supervisor-only utilities into this directory during installation. This directory cannot be deleted.

System supervisor

See **SUPERVISOR; User.**

TTT

Tape backup unit

An external tape drive that backs up data from hard disks.

See also **Back up; Backup.**

Terminal emulation software

Software that duplicates the communication protocol of a dedicated terminal, giving workstation users a connection to the DG/UX environment. A workstation running terminal emulation software acts as if it were wired directly to the AViiON system's terminal ports. NetWare's terminal emulation driver, NVT, interacts with the IPX/SPX driver to send and receive data from the NetWare workstations. NVT combined with a third-party terminal emulation program processes the given protocols and routes the characters either to the AViiON system through the host terminal driver or to the workstation through the IPX/SPX driver.

Traditionally, intelligent workstations using terminal emulation are connected asynchronously to the host. With NetWare, workstations using terminal emulation are connected via the network, greatly increasing the performance of terminal emulation as well as simplifying the installation of terminal lines.

NetWare supports a variety of third-party terminal emulation programs, such as Reflections, Smarterm, and Dynacomm.

See also **NVT.**

Terminating resistor

A grounding resistor placed at the end of a bus, line, chain, or cable to prevent signals from being reflected or echoed. Sometimes shortened to "terminator."

Termination

See **SCSI bus.**

Topology

The physical layout of network components (cables, network stations, gateways, hubs, etc.). The three basic interconnection topologies include star, ring, and bus networks. On a star network, workstations are connected directly to a file server but not to each other. On a ring network, the file server and workstations are cabled in a ring; a workstation's messages may have to pass through several other workstations before reaching the file server. On a bus network, all workstations and the file server are connected to a central cable (called a trunk or bus).

Trustee rights

A method which controls the directories and files a user or group can access and what a user or group is allowed to do in them. A trustee assignment consists of the rights assigned to a particular user or group. A user or group who has been assigned rights to work in a directory or file is known as a "trustee" of that directory or file.

Automatic Assignment. If you make a trustee assignment in a directory, the trustee has access to the directory, its files, and its subdirectories (unless the rights are redefined at the file or subdirectory level). In other words, trustee rights "flow down" through the structure unless

- Other trustee assignments are granted at a lower level of the directory structure, or
- The Inherited Rights Mask of a subdirectory or file revokes rights assigned in a trustee assignment.

Default Rights. When you make a trustee directory assignment, the default rights (Read and File Scan [RF]) allow a trustee to read the files in the directory and to see the subdirectories and files in the directory. Any trustee assignment, whether for directories or files, also includes the right to see the path leading from the root to that directory or file.

A new assignment of trustee rights at the file level can either revoke rights assigned at the directory level or allow additional rights.

SUPERVISOR Trustee Rights. The user SUPERVISOR has all rights in all directories and files and can assign any of these rights to users and groups.

A trustee must have the Access Control right [**A**] before making trustee assignments in a directory or file.

Rights security is controlled by both trustee assignments and the Inherited Rights Mask (IRM). When you grant a trustee assignment, it takes precedence over the IRM in the current directory. However, in the subdirectories, the Inherited Rights Mask takes precedence, unless new trustee assignments are granted. Both the trustee assignment and the IRM use the same rights.

Some common tasks and the rights required to do them are listed in the following figure.

Task	Rights required
Read from a closed file	Read
See a filename	File scan
Search a directory	File scan
Write to a closed file	Write, Create, Erase, Modify
Create and write to a file	Create
Copy or NCOPY files into a directory	Create
Remove an empty subdirectory	Erase
Delete a file	Erase
Change directory or file attributes	Modify
Rename a file	Modify
Change the Inherited Rights Mask	Access Control
Change trustee assignments	Access Control
Modify a directory's disk space assignment between users	Access Control

To grant or modify a trustee assignment for either directories or files, use **ALLOW; FILER; GRANT; REMOVE; REVOKE; SYSCON** (*Utilities*).

See also **Rights; Security.**

UUU

User

Any person allowed to work on the network. Each person needs a user identity, or username, to work on the network. Once a username exists as an object in the file server bindery, the user can then log in with that username and access the network. Although any number of users can be created, only 250 users can be logged in simultaneously to a file server running NetWare for AViiON, depending on user count.

You can simplify user access to file server resources (such as applications, printers and print queues, or directories) by creating groups on the file server and giving groups access to resources. Once a group is created, you can assign users; as members of the group, users inherit the group's privileges.

System-Created Users and Groups

Two usernames and a group already exist in the file server bindery when the file server is installed:

- SUPERVISOR is the username for the network supervisor or system administrator.
- GUEST is the username for anyone who needs temporary and restricted access to the file server.
- EVERYONE is the group that includes all users.

SUPERVISOR has all rights in all directories. These rights cannot be revoked, nor can user SUPERVISOR be deleted or renamed. Because user SUPERVISOR initially has no corresponding password, the network supervisor can log in to the file server when setting up the network environment. SUPERVISOR is a user bindery object with ID Number 1.

For maximum security, consider the following.

- Set a supervisor password in SYSCON the first time you log in as SUPERVISOR. Change this password regularly and do not select an obvious password, such as a spouse's name.

- Create a second username to use when you work on the network as a regular user. Log in as SUPERVISOR only when you have supervisor tasks to perform.

- Set up a "back door" to the system in one of two ways:

  1. Create a fictitious user with an unpredictable (but unforgettable) username and make that user security equivalent to SUPERVISOR.

  2. Create a fictitious user with an unpredictable (but unforgettable) username and make that user the user account manager for both the fictitious user and SUPERVISOR.

- Use caution in making anyone security equivalent to SUPERVISOR. Instead, delegate supervisor jobs by designating operators and managers.

GUEST is a user-type bindery object and serves as a username for anyone who needs temporary and restricted access to the file server.

GUEST is a member of the group EVERYONE, and GUEST's rights flow from membership in that group. GUEST has no password, but you can require a password on GUEST's account.

You can delete GUEST from the file server, or you can remove GUEST from group EVERYONE and assign specific rights to GUEST.

If you want GUEST to have personal workspace, create a GUEST directory and assign rights to GUEST.

For maximum security, consider the following.

- Require a password on GUEST's account. Assign GUEST a password in SYSCON and change it frequently. Do not allow GUEST to change the password.

- Delete GUEST from group EVERYONE and make a specific trustee assignment to GUEST, such as EVERYONE's rights to SYS:PUBLIC and the DOS directories. You can also grant rights to whichever application and files you permit GUEST to use or view.

- Delete GUEST from the file server if you have no temporary users.

EVERYONE is a group that includes all users created on the file server. EVERYONE is assigned Read and File Scan rights in the SYS:PUBLIC directory and Create rights in SYS:MAIL. The network supervisor can delete any user from group EVERYONE or change EVERYONE's trustee rights in any directory (including rights granted by the system).

Do not remove EVERYONE's trustee assignments to the SYS:PUBLIC and SYS:MAIL directories. If you do, users cannot access NetWare utilities or send electronic mail.

EVERYONE is a User Group bindery object. Although EVERYONE can be deleted from the file server, we do not recommend doing so. If group EVERYONE is deleted and then re-created, existing users must be added to the group one at a time.

Other Users and Groups

When you set up the network environment, you can define

- Regular network users: the persons for whom you create usernames and user accounts;

- Groups: collections of network users who share applications, perform similar tasks, or have similar needs for information;

- Managers and Operators: users to whom you assign certain supervisor rights and responsibilities for system administration.

See **User accounts** for detailed information regarding regular network users, groups, and managers and operators.

User account

Part of network security that controls the user environment. Some features of user accounts are assigned to each user; some must be created or assigned; and some are optional.

Usernames can be up to 47 characters but, for efficiency, a username for DOS workstations is usually 8 characters and follows one of the following formats.

- Given name (for example, user JANE and user RICHARD)
- Surname (for example, user DOE and user SMITH)
- Initials and surname (for example, user JDOE and user RDSMITH)

If you choose to assign initials and surname, you are less likely to have problems with duplicate names.

The username is also the login name and must be supplied when logging in. As SUPERVISOR, you can record the user's full name for your own information.

You can view a list of existing users with SYSCON's "User Information" option. When you select a particular username from that list, you can also view the user's account features and restrictions.

Group membership. Users are assigned to group EVERYONE and inherit the rights assigned to that group. Other groups are created in SYSCON as empty sets and then users are assigned or added. Group members inherit the rights assigned to groups.

By selecting a particular username from SYSCON's list of users, you can view a list of "Groups Belonged To." You can also view a list of existing groups with SYSCON's "Group Information" option. When you select the name of a particular group from the "Group Information" list, you can view the group's "Member List."

Home or username directories are optional. The home or username directory serves as personal workspace. To have a home or username directory, plan a parent directory (such as SYS:HOME or SYS:USERS) for these directories. For a large system, you may prefer to set aside a separate volume for username directories.

For login script purposes, each user's home directory name should be the same as that user's username (for example, SYS:USER/JANE or SYS:HOME/RDSMITH).

If you grant all trustee rights to users in their own username directories, each user can then control access to files in the home directory. Users, however, cannot restrict SUPERVISOR, who has all rights to all directories.

Users can use their username directories to create files and work on projects without allowing other users to have access to their work. Once the work is completed, the files can be copied to a work or project directory (group workspace) where other users have rights to access the information.

However, if you prefer to have work done in work or project directories, you can restrict the disk space in username directories.

The USERDEF utility creates username directories in volume SYS at the time users are created unless you create and specify a parent directory for username directories. When username directories are created by the system, trustee assignments are also made.

Trustee assignments. For users to have access to specific directories and files (other than those assigned by the system), you must make trustee assignments. You can assign users trustee rights to specified directories and files. You can view trustee directory assignments or trustee file assignments for any user by selecting that username from the list of users under SYSCON's "User Information" option.

Security equivalences. With a security equivalence, a user is allowed to exercise rights equivalent to those of another user. Assigning a security equivalence is convenient when you need to give a user temporary access to the same information another user has access to. In networks containing confidential data that only selected users have access to, take care that you do not inadvertently give a user access to restricted information. Use caution in assigning Supervisor equivalence. Delegate responsibilities to managers and operators instead. You can view security equivalences by selecting a username from the list of users under SYSCON's "User Information" option.

ID numbers are random, hexadecimal numbers assigned by the file server to each bindery object (including users).

As user SUPERVISOR, you can view an ID number for an existing user by selecting the user from SYSCON's list of existing users and then selecting the "Other Information" option.

Mailboxes in the SYS:MAIL directory contain user login scripts and print job configurations. Each user has a mailbox directory named with the user's ID number. Users have all but the Supervisory right in this directory. Because users' login scripts are stored in their mailbox directories, never delete SYS:MAIL or any of its subdirectories, even if you are not using electronic mail.

User login scripts are configurable batch files that customize the network environment for individual users by initializing environment variables, mapping drives, and executing other commands.

You can view a user's login script by selecting that user from SYSCON's list of existing users and then selecting the "Login Script" option. If users are allowed to change their own passwords, they can also change their own login scripts.

Print job configurations. Each user can use printing defaults. Or you can create print job configurations in PRINTCON and copy from one user to others. Print job configurations are stored in each user's mailbox directory in SYS:MAIL.

Account management. SUPERVISOR manages the accounts of all users. If users are created by a Workgroup Manager, then the Workgroup Manager can manage these user accounts. You can

assign existing users to a User Account Manager, who can be either a Workgroup Manager or any other user. You can also have more than one manager for a user account.

You can determine which user or group manages an existing user's account by selecting that user from SYSCON's list of existing users and then choosing the "Managers" option. If a user (or group) manages other user accounts, you can also view a list of managed users and groups in SYSCON's "User Information" by selecting the manager's username and then selecting "Managed Users and Groups."

Login restrictions are assigned at the account level to make it difficult for unauthorized users to access the file server. When certain limits are exceeded, an account is disabled. When an account is disabled, no one can log under that username.

You can restrict logins in the following ways:

- **Account Balance.** If you have installed Accounting to monitor or limit network resources, you can assign initial account balances for users and specify credit limits. When the account balance is depleted, the account is disabled.

  To view the account balance for a particular user, select that user from SYSCON's list of existing users and select "Account Balance." If you have not installed accounting, this option does not appear on the "User Information" menu.

- **Expiration.** You can specify an expiration date for a user account. The account will expire at 12:01 a.m. the following day. Any attempt to log in after the account expires will disable the account. The default is no expiration date.

  To view an account expiration date, select a particular user from SYSCON's list of existing users and select "Account Restrictions."

- **Password.** You can require a password. You can also specify the minimum length of passwords (the default is five characters), how often the password must be changed (the default is every 40 days), whether the password must be unique (the default is No), and whether the user can change the password (the default is Yes). For a password to be unique, it must be different from the previous ten passwords used by the account.

You can also specify the number of times a user can log in with an expired password or the number of incorrect login attempts (the default is six times). When that number is exceeded, the account is disabled.

To view password specifications, select a particular user from SYSCON's list of existing users and select "Account Restrictions."

If you allow users to change passwords, you also allow them to edit their own login scripts.

Disk Space Restrictions. You can limit the amount of disk space for each user by specifying the maximum number of blocks available for each user per volume. The size of the block depends on the default allocation size selected during installation.

To view the volume restrictions for each user, select that particular user from SYSCON's list of existing users and select "Volume Restrictions."

Connection Restrictions. You can limit the number of workstations a user can log in from concurrently. You can specify the maximum number of concurrent connections permitted.

To view concurrent connection limitations for a user, select that particular user from SYSCON's list of existing users and select "Account Restrictions."

Time Restrictions. You can restrict the hours during which users can log in. Hours are specified in half-hour blocks. You can assign all users the same hours, or you can restrict users individually.

To view the time restrictions for a user, select that particular user from SYSCON's list of existing users and select "Time Restrictions."

Station Restrictions. You can restrict the physical locations that a user can log in from by specifying the network and node addresses of the workstation the user is permitted to log in from.

Station restrictions cannot be set with system default restrictions; they must be assigned individually. To view the workstations a user is limited to, select that particular user from SYSCON's list of existing users and select "Station Restrictions." If the "Allowed Login Addresses" box is empty, no station restrictions are in effect.

Utilities for Creating Users

You can create network users with the SYSCON, MAKEUSER, and USERDEF utilities. Groups, however, can be created only in SYSCON. No matter what utility you use to create users, you can use only SYSCON to modify existing user accounts.

SYSCON. You can create users individually with the "User Information" option. By setting the System Default Restrictions, you assign all login restrictions except station restrictions to new users. Any features of user accounts not created by defaults must be individually created or assigned.

MAKEUSER. You can create multiple users by creating and processing a .USR script with MAKEUSER. A .USR script is a list of commands in a text file that specify how to create users and user account features (such as group memberships, passwords, and time restrictions).

MAKEUSER, however, does not support trustee file rights; you can assign trustee rights to directories, but not to files.

You can create a .USR script by using the cut and paste features of a text editor or by typing the script in the MAKEUSER script box. All commands in the .USR script must be entered in a specific order.

USERDEF. You can create multiple users with similar characteristics with USERDEF. Instead of creating a .USR script in MAKEUSER, you can use a template that allows you to specify the same parameters. When you have entered all the usernames, USERDEF creates users by creating a temporary .USR script and then MAKEUSER processes it. USERDEF also does not support trustee file rights; you can assign trustee rights to directories, but not to files.

When users are created with the defaults provided in USERDEF, each new user is provided a basic login script with the essential drive mappings. The first search drive is mapped to SYS:PUBLIC and the second to the appropriate DOS directory. The first network drive is mapped to the user's default directory. Although these mappings make it possible to work on the network right away, these mappings are more appropriate for a system login script.

USERDEF also supplies new users with an initial password and SUPERVISOR's print job configurations so that new users can begin work on the network.

You can also customize the way USERDEF creates new users by creating a custom template. To do this, set new default parameters or edit the basic login script.

Although users created with USERDEF can begin work on the network immediately, consider using USERDEF only in two instances:

- If you must get large numbers of new users on the network quickly, use the default template for users.
- If you want to create users in batches, but do not want to plan MAKEUSER scripts, create a custom template for users.

See also **Accounting; Groups; User Account Manager; Workgroup Manager.**

Related utility: **SYSCON** (*Utilities*).

User Account Manager

The user or group member who has rights to manage user accounts and groups. Existing users can be assigned to a Workgroup Manager or to any other user or group for account management. Workgroup Managers are User Account Managers for users they create. Even though account management is delegated, SUPERVISOR still has all rights to manage user accounts.

User Account Managers can

- Delete managed users and groups;
- Assign a managed user to a managed group;
- Assign a managed user as User Account Manager.

User Account Managers can also modify all options in SYSCON's "User Information" submenu not requiring file rights, including

- Account Balance
- Account Restrictions
- Change Password
- Full Name
- Groups Belonged To (if the groups are managed groups)
- Login Script
- Managed Users and Groups
- Managers
- Security Equivalences
- Station Restrictions

User Account Managers must be assigned file rights in the directory structure before they can make or modify

- Trustee directory assignments
- Trustee file assignments
- Volume restrictions
- Disk space restrictions

User Account Managers cannot

- Create users or groups;
- Assign managed users to a group the manager does not manage;
- Modify the login restrictions of their own accounts (unless they are also assigned management of their own accounts).

Why have User Account Managers? By assigning experienced users as User Account Managers, especially in a large system, they can handle routine tasks such as assigning users to new groups or changing drive mappings (in individual login scripts), account restrictions, account balances, and so on.

The User Account Manager can be in charge of a workgroup, if you wish. But even if you do not organize workgroups, you can delegate these responsibilities to User Account Managers.

A user can be managed by more than one user account manager. By assigning a group or two or more User Account Managers to manage the same users and groups, you have a backup if one of the User Account Managers is not available.

See also **User**; **Workgroup Manager**.

Related utility: **SYSCON** (*Utilities*).

Utilities

NetWare programs that let you perform tasks such as adding users, and assigning rights. The NetWare utilities are divided into groups according to where the commands to enter the utilities are executed: file server utilities, workstation utilities, and router utilities.

File Server Utilities

The file server utility for NetWare for AViiON Systems is SCONSOLE. This utility is documented further in the *System Administration* manual.

SCONSOLE is used by the system supervisor to configure and administer the NetWare file server, which is part of the AViiON system. SCONSOLE is a menu-driven utility, and runs as a DG/UX process.

See also **SCONSOLE**.

Workstation utilities

NetWare workstation utilities are designed to change the network after initial installation or to perform network tasks. The two types of workstation utilities include command line utilities and menu utilities. These utilities are documented in the *Utilities* manual.

Command line utilities are executed at the workstation. You can use these utilities to manipulate rights and attributes, copy and print files, log in and out, view file server information, and map network drives. Once you are familiar with command line utilities, you will find them faster to use than menu utilities.

Rights/ Attributes	Directories/ Volumes	Server
ALLOW	CHKDIR	NVER
FLAG	CHKVOL	PAUDIT
FLAGDIR	DSPACE	SECURITY
GRANT	LISTDIR	SETPASS
REMOVE	MAP	SLIST
REVOKE	RENDIR	SMODE
RIGHTS	VOLINFO	SYSTIME
TLIST		VERSION

Users	Files
CASTOFF	NBACKUP
CASTON	NCOPY
HELP	NDIR
SEND	PURGE
USERLIST	
WHOAMI	

Menu utilities allow you to perform network tasks by choosing options from menus. You can complete some tasks such as creating users only in a menu utility. The utilities are designed so that some options are available only to SUPERVISOR, to users designated as Supervisor-equivalent, or to operators. Menu utilities make it easier to remember how to complete tasks by displaying options.

- **COLORPAL.** Use to modify the color schemes for NetWare menu utilities.

- **FILER.** Use to view and modify volume, directory, and file information. You can grant and revoke trustee assignments, as well as assign and modify directory and file attributes.

- **MAKEUSER.** Use to create large groups of users. MAKEUSER is particularly useful to system supervisors who must regularly create and delete large groups of users.

- **SESSION.** Use to perform a variety of network tasks. SESSION combines the functions of several command line utilities into a single menu utility.

- **SYSCON.** Use to create users and groups, specify Workgroup and User Account Managers, and designate trustee assignments.

- **USERDEF.** Use to create and define templates and then create large groups of users. USERDEF works in conjunction with MAKEUSER.

Router Utilities are executed at the router console to monitor and regulate the router's resources. You can run Value-Added Processes (VAPs) on the router. The following router commands are documented in the *NetWare 286 External Routers Supplement*.

CONFIG
CONSOLE
DOS
DOWN
MONITOR
OFF

VVV

Value-Added Process

See **VAP**.

Value-added server

A separate, specialized, dedicated computer (such as a print server or a database server) that fulfills a specific function for network users.

See also **VAP**.

VAP

(Value-Added Process) A program that runs "on top" of the NetWare v2.*x* network operating system (in much the same way a word processing or spreadsheet application runs on top of DOS). VAPs tie in with the network operating system so additional enhancements can provide services without interfering with the network's normal operation. VAPs must be run on a NetWare v2.*x* external router or a NetWare v2.*x* file server.

Volume

A point in the DG/UX operating system directory structure where the NetWare volume begins. The first network volume is named SYS, and contains the SYSTEM, PUBLIC, LOGIN, MAIL, and DELETED.SAV directories.

Several NetWare utilities, including MAP and VOLINFO, list a file server's volume names in one form or another. In addition, the DOS DIR command lists the volume name for the specified network drive (for example, "Volume in drive F is SYS"). This corresponds to the DOS volume label shown by the DOS DIR command for local disks (floppy disks or workstation hard disks). (A local disk can be given a volume label during formatting or with the DOS LABEL command.)

When a volume is used as part of a directory path, either in NetWare documentation or on the screen (for example, when running the MAP command), the volume name is followed by a colon (:), as in SYS:PUBLIC.

The *volume* token in the NWConfig file is used to assign NetWare volumes to directories on the host disk system. For example, by specifying *volume = SYS:/nw/sys*, the NetWare volume SYS: is mapped to the host path */nw/sys*.

See also **Directory structure.**

WWW

Wait state

A period of time when the processor does nothing; it simply waits. A wait state is used to synchronize circuitry or devices operating at different speeds. For example, wait states used in memory access slow down the CPU so all components seem to be running at the same speed.

Watchdog process

Part of the NetWare daemon that monitors connections. If a client application is hung or if the machine suffered a power outage or was turned off, the watchdog on the AViiON waits five minutes and sends a packet to the client that asks, "Are you there?" If the client doesn't respond, the NetWare daemon waits for five minutes before sending another packet.

If the client doesn't respond to the first packet, the NetWare daemon sends another packet, and will continue sending packets at one-minute intervals until a total of eleven watchdog packets are sent. If a client fails to respond to all eleven packets, the NetWare daemon terminates the connection, closes open files, and makes the connection available for another client. This process takes about fifteen minutes.

Configure the watchdog process using the Forced Logout parameter in SCONSOLE.

WAN

See Wide area network.

Wide area network

A network that communicates over a long distance, such as across a city or around the world. A local area network becomes a part of a wide area network when a link is established (using modems, remote routers, phone lines, satellites, or a microwave connection) to a mainframe system, a public data network, or even to another local area network.

Workgroup Manager

An assistant network supervisor with rights to create and delete bindery objects (such as users, groups, or print queues) and to manage user accounts. A Workgroup Manager has supervisory privileges over a part of the bindery. When several groups share a file server, use Workgroup Managers over groups that want autonomous control over their own users and data.

Workgroup Managers supplement, but do not replace, the network SUPERVISOR. Workgroup Managers can manage only those users and groups they create or those assigned to them for account management (by designating a Workgroup Manager as the User Account Manager). SUPERVISOR retains absolute control over the network.

Workgroup Managers do not automatically acquire rights to the directory structure and file system. These rights must be granted by SUPERVISOR. Consider assigning Workgroup Managers the Supervisory right in a specific volume or directory so that they can grant directory and file rights to users in their workgroups. Also, if you assign file rights to a directory (rather than to a volume), consider making a disk space assignment to the directory.

Workgroup Managers can

- Create users and manage their accounts;
- Delete users they have created;
- Create groups and add users they manage.

Workgroup Managers must be assigned file rights before they can make or modify

- Trustee directory assignments;
- Trustee file assignments;
- Volume restrictions;
- Disk space restrictions.

Workgroup Managers cannot

- Create a user and make that user security equivalent to SUPERVISOR;
- Create a Workgroup Manager;
- Manage users or groups they have not created unless also designated as the User Account Manager;
- Assign any rights they have not been assigned by SUPERVISOR;
- Modify the login restrictions of their own accounts (unless they are also assigned management of their own accounts);
- Create or delete print queues.

Designating a Workgroup Manager. A Workgroup Manager may be either a user or a group. If the Workgroup Manager is a user, the manager must first be created as a user in SYSCON's "User Information." If the Workgroup Manager is a group, the group must first be created in SYSCON's "Group Information." If you designate a group as Workgroup Manager, each member of the group will have Workgroup Manager privileges. By using a group you can change the assignment when you add or delete group members.

Workgroup Manager is not a bindery object. A set property called MANAGERS is added to the SUPERVISOR object. Any object (user or group) that is security equivalent to an object listed in the MANAGERS property set is considered to be a Workgroup Manager. When a Workgroup Manager creates users, the bindery uses the Workgroup Manager's ID number to indicate that the Workgroup Manager becomes the User Account Manager for these users.

The Workgroup Manager concept is two-tiered: SUPERVISOR creates Workgroup Managers, and Workgroup Managers create and manage users. However, Workgroup Managers cannot create other Workgroup Managers. You can create more complex relationships by controlling the place and level in the directory structure where Workgroup Managers are given rights. This placement can effectively create hierarchical relationships through the data the Workgroup Managers control.

For maximum security,

- Specify passwords in SYSCON for all Workgroup Managers' accounts.

- Require Workgroup Managers to create a second username to use when working on the network as regular network users. They should log in under the Workgroup Manager username only when performing management tasks.

- Use caution in making anyone security equivalent to a Workgroup Manager.

User Account Manager. When a workgroup is reorganized or a system is upgraded, users and groups can be assigned to a Workgroup Manager (or any other user or group) for account management. The user who manages a reassigned user, whether a Workgroup Manager or another user or group, is called a User Account Manager. If a group is assigned as User Account Manager, a user may have more than one manager, but you can also assign an account to two or more users.

As network supervisor, you can assign users to workgroups when you create users if you first create usernames for Workgroup Managers and then designate these users as Workgroup Managers.

Or you can create a group called MANAGERS, create the prospective members as users, and then assign them to the group.

To determine who manages a user's account, select that user from SYSCON's list of existing users and choose the "Managers" option. Although SUPERVISOR has all rights to create and delete users and modify user accounts, SUPERVISOR is not listed with "Managers."

By selecting the username of the Workgroup Manager or User Account Manager and then selecting "Managed Users and Groups," you can also view a list of managed users and groups in SYSCON's "User Information" menu option.

See also **SUPERVISOR; User; User Account Manager.**

Related utility: **SYSCON** (*Utilities*).

Workstation

A personal computer connected to a network and used to perform tasks through application programs or utilities.

Workstation boot files

See **Boot files.**

Workstation shell

See **NetWare shell.**

Write right

See **Rights; Security (Rights Security).**

XXX

XMSNETX.EXE

The NetWare extended memory shell program that works with IPX, SPX, and a LAN driver to convert a standalone computer into a network workstation. Loaded into RAM each time a workstation boots, XMSNETX.EXE begins network transmission each time a workstation requires service on the network.

See also **BNETX.COM; EMSNETX.EXE; NETX.COM; NetWare extended memory shell.**

XON/XOFF

See **Serial communication.**

INDEX

C

D

E

F

G

H

M

N

O

P

Q

R

S

T

U

V

W

X

NetWare® for
AViiON® Systems:
Concepts

069–000483–01

Cut here and insert in binder spine pocket