Contents

How to Use This Manual

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z

Preface

How to Use This Manual

Introduction

Concepts is an extended glossary of terms related to the NetWare® network operating system. Use this manual as a reference if you have questions during the installation and operation of your network.

Concepts are arranged alphabetically. Some entries contain See or See also references to other entries where concepts are explained in detail. Some entries refer you to related information in other manuals.

Note

In Novell documentation, an asterisk denotes a trademarked name belonging to a third-party company. Novell trademarks are denoted with specific trademark symbols, such as TM.

Chapter 1 A

Abend

(Abnormal end) A message issued by the operating system when it detects a serious problem, such as a hardware or software failure. The abend stops the NetWare® server.

Abend messages are explained in *System Messages* . What to do when you get an abend is explained in Troubleshooting the Network in *Supervising the Network* .

Access Control List

(ACL) An object property that stores information about who or what can access that object.

An ACL contains trustee assignments that include object and property rights. The ACL also contains the Inherited Rights Filter. When you view an object's trustees or its Inherited Rights Filter, you are seeing the *values* of that object's ACL.

An ACL for an object is like the list of trustees for a file or directory.

To change an ACL (and therefore a trustee's rights to an object), you must have a property right that allows you to modify the ACL for that object.

See also "Object" ; "Security."

Access Control right

A file system right that grants the right to change the trustee assignments and Inherited Rights Filter of a directory or file.

See “Rights.”

Accounting

The process of tracking resources used on a network.

The network supervisor can charge for network services and resources by assigning users account balances that they draw from as they use the services and resources.

Charging for Network Services and Resources

The network supervisor can assign different charge rates for services at different times of the day, in half-hour increments.

The network supervisor can set up charges for

- **Blocks read** is the charge amount is for each block of data read from the server.
- **Blocks written** is the charge amount is for each block of data written to the server.
- **Connect time** is the charge amount is for each minute a user is logged in. User logins and logouts are tracked automatically.
- **Disk storage** is the charge amount is for each block of data stored on the server's disk for one day.
- **Service requests** is the charge amount is for each request to the server.

To calculate the charge rate for services, the supervisor should

- Determine network costs and the amount to charge over a given period of time.
- Decide which services to charge for (based on network costs) and determine the amount needed to cover the costs of each service.

  For example, if server disk storage capacity is a concern, then charge for disk storage. If network use is high, charge for service requests. To

encourage users to log out when they aren't working, charge for connect time.

- Estimate how much each service is being used by monitoring the server for two or three weeks.

  For example, if 30% of the server's charges are from service requests, the supervisor would want to recuperate 30% of network costs by charging for service requests.

  At the end of the monitoring period, use ATOTAL to determine total use of each service. (ATOTAL is located in SYS:SYSTEM and requires supervisor rights.) See ATOTAL in *Utilities Reference* .

After establishing how much each service is used and the amount needed to cover the cost of each service, the supervisor can calculate a charge rate.

The charge rate is the charge per unit of the specified service. This rate converts the amount of service used to a monetary figure. The unit is arbitrary, but consider beginning with one charge unit equaling one cent.

Use the following formula to calculate a charge rate:

$$\frac{\textbf{CHARGE}\ \text{(charge rate multiplier)}}{\textbf{ESTIMATED USAGE}\ \text{(charge rate divider)}} = \textbf{CHARGE RATE}$$

For example, a network supervisor needs to charge $100 per month for blocks read. There are 250,000 blocks read each month. Therefore, the charge rate is $100 (or 10,000 cents) divided by 250,000 blocks, or $.01 (1 cent) per 25 blocks:

$$\frac{\textbf{10,000}\ \text{cents}}{\textbf{250,000}\ \text{blocks read}} = \textbf{1}\ \text{cent}\ \textbf{/ 25}\ \text{blocks read}$$

Assigning Account Balances

The network supervisor can

- Assign each user a balance to limit the amount of services a user can use

- Assign a credit limit (or allow unlimited credit)
- Assign a default account balance for all users
- Increase a user's account balance

The user must log out and log in again before changes take effect.

Related utilities: NETADMIN and NetWare Administrator in *Utilities Reference* .

ACL

(Access Control List) An object property that stores information about who or what can access that object.

See also “Access Control List”

Active hub

A device that amplifies transmission signals in network topologies.

See also “Hub.”

Add or Delete Self right

A property right that grants a trustee the right to add or remove itself as a value of the property.

See also “Rights.”

Address

A number that identifies a location in memory or disk storage or that identifies the location of a device on the network.

See “IP address” ; “Network numbering.”

Address Resolution Protocol

(ARP) A process in Internet Protocol (IP) networks that allows a host to find the Media Access Control (MAC) address of a target host on the same physical network when it only knows the target's IP address.

With ARP, a network board contains a table that maps IP addresses to the hardware addresses of the objects on the network.

To create entries, the ARP broadcasts a request with the target's IP address. The target responds with its physical address. The network board adds the physical address to its ARP table and can then send packets to the target.

Alias object

A leaf object that points to the original location of an object in the Directory. Aliases can make Novell® Directory ServicesTM (NDS) easier to use.

Any Directory object located in one place in the Directory can also appear to be in another place in the Directory by using aliases.

For example, an administrator could create aliases pointing to all the modems on the network. The aliases could be created in one container. A user would then need to search only one area of the Directory to find all modems on the network.

However, when you move or rename a container object in a Directory tree, you have the option of creating an alias in place of the moved or renamed object. If you select this option, NDSTM features automatically create the alias for you and assign it the same name as the original object.

Creating an alias in place of a moved or renamed container object allows users who are unaware of the object's new location to see the object in its original Directory location.

When you add aliases to a list (for example, adding an alias of a user to a group) the name of the object appears in the list, not the name of the alias that points to the object.

To access the alias and the properties of the object it refers to, you need the Read right to the alias name and the Read right to the properties of the object it refers to.

See also “Object” ; Creating Leaf Objects and Cautions When Deleting Alias Objects in *Supervising the Network* .

Application object

A leaf object that represents a network application in the Novell Directory tree. Application objects allow you to manage the network more efficiently, saving time in administering applications. Application objects simplify administrative tasks such as assigning rights, customizing login scripts, and supporting applications.

Archive

A transfer of files to long-term storage media, such as optical discs or magnetic tape.

See also “Attributes” ; “Backup” ; “Data migration” ; “High Capacity Storage System” ; “Storage Management Services.”

Archive Needed (A) attribute

A file attribute, set by the NetWare operating system, indicating that the file has been changed since the last time it was backed up.

See also “Attributes.”

ARP

(Address Resolution Protocol) A process in IP networks that allows a host to find the MAC address of a target host on the same physical network when it only knows the target's IP address.

See also “Address Resolution Protocol.”

Attach

Establishes a connection between a workstation and a NetWare server.

In networks running NetWare 3TM or earlier versions, users connected to multiple file servers using the ATTACH command. In NetWare 4, with Novell Directory Services, users no longer need to attach separately to multiple servers.

When users log in to the Directory tree, they automatically have access to any resources in the Directory tree to which they have rights. Rights to resources are verified through authentication.

In NetWare 4, the ATTACH command can still be used in login scripts to establish connections with bindery-based servers.

Related utilities: LOGIN , LOGOUT , and MAP in *Utilities Reference* .

See also “Authentication” ; “Novell Directory Services.”

Attributes

The characteristics of a directory or file. In NetWare, these characteristics are called flags.

NDS objects do not have attributes.

Attributes dictate what can be done with a file or directory. For example, you can set a file to be a Read Only (Ro) file.

While the term attributes is used predominantly for DOS files, NetWare offers additional attributes, and then applies them to both files and directories.

Table 1-1 File Attributes

Attribute	Description
Archive Needed (A)	A status flag set by NetWare.Indicates that the file has been changed since the last time it was backed up. NetWare sets this attribute when a file is modified. Backup programs usually clear this attribute after backing up the file.
Can't Compress (Cc)	A status flag set by NetWare. Indicates that the file can't be compressed because of insignificant space savings. This attribute is shown on attribute lists, but can't be set by the user.
Compressed (Co)	A status flag set by NetWare. Indicates that the file is compressed. This attribute is shown on attribute lists, but can't be set by the user.
Delete Inhibit (Di)	Prevents any user from erasing the file.
Don't Compress (Dc)	Marks the file so that it is never compressed.
Don't Migrate (Dm)	Marks the file so that it is never migrated to a secondary storage device (such as a tape drive or optical disc).
Don't Suballocate (Ds)	Prevents an individual file from being suballocated, even if suballocation is enabled for the system. Use for files that are enlarged or appended frequently, such as certain data base files.
Execute Only (X)	Prevents a file from being copied. Only the Supervisor can set this file attribute; it *cannot* be cleared. It should be set only if you have a second copy of the file. Backup utilities don't back up a file marked Execute Only, and some program files with this attribute set don't execute properly.
Hidden (H)	Hides the file from the DOS command and prevents it from being deleted or copied. However, the NetWare NDIR command shows the file if the user has the File Scan right. (See also "Rights.")
Immediate Compress (Ic)	Marks the file so that it is compressed on disk as soon as the operating system can do so, without waiting for a specific event to initiate compression (such as a time delay).
Migrated (M)	A status flag set by NetWare. Indicates that the file is migrated. This attribute is shown on attribute lists, but can't be set by the user.
Normal (N)	No file attributes are set.

Attribute	Description
Purge (P)	Tells NetWare to purge the file when it is deleted. The file can't be salvaged with the FILER utility.
Read Only (Ro)	Indicates that no one can write to this file. When Read Only is set or cleared, NetWare also sets or clears the Delete Inhibit and Rename Inhibit attributes. Consequently, a user can't write to, erase, or rename a file when Read Only is set. A user with the Modify right can remove the Delete Inhibit and Rename Inhibit attributes without removing Read Only. Then the file can be deleted or renamed, but not written to. (See also "Rights.") NetWare shows Read Write (Rw) if Read Only isn't set.
Read Write (Rw)	Allows users to change the content of the file. Assigned by default when Read Only is not set.
Rename Inhibit (R)	Prevents a user from renaming a file.
Shareable (Sh)	Allows the file to be accessed by more than one user at a time. Usually used in combination with the Read Only attribute.
System (Sy)	A DOS attribute. Marks a file used only by an operating system. The file is hidden from the DOS command and can't be deleted, renamed, or copied. However, the NetWare NDIR command shows the file if the user has the File Scan right. (See also "Rights.")
Transactional (T)	Indicates that the file is protected by Transaction Tracking System (TTS). TTS™ prevents data corruption by ensuring that either all changes are made or no changes are made when a file is being modified. Set this attribute for all database files you want protected by TTS. (See also "Transaction Tracking System.")

Set or clear attributes with the FLAG command line utility, the FILER menu utility, or the NetWare Administrator graphical utility.

Related utilities: FILER , FLAG , NETADMIN , and NetWare Administrator in *Utilities Reference* .

Auditing

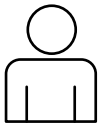
The process of examining network transactions to ensure that network records are accurate and secure.

In general, auditing means examining records to make sure that transactions are accurate and that confidential information is secure.

NetWare auditing allows individuals, acting independently of network supervisors and other users, to audit network transactions.

Auditors can audit NDS events as well as those events specific to a volume or a server. Some events you can audit are shown in the following figure.

Figure 1-1
Audited Events



File or directory events

- Create, modify, delete directories or files
- Salvage, move, rename directories or files
- Create, delete, service queues

Server events

- Down server
- Create, delete bindery objects
- Mount, dismount volumes
- Modify security rights

Directory Service events

- Add, delete objects
- Move, rename objects
- Add, remove security equivalence
- Track User object logins and logouts

Auditors can track events and activities on the network, but they don't have rights to open or modify network files (other than the audit data and audit history files), unless they are granted rights by the network supervisor.

Auditing is enabled at the volume level for file system auditing. It is enabled at the container level when auditing NDS events.

Note

The Audit program files are installed automatically when you install or upgrade to NetWare 4.

Audit data and history files are automatically created for volumes and containers that have auditing enabled. The files keep records much like a system or error log file. All activity tracked by the auditing utility is recorded.

The audit files continue to accept records until auditing is disabled or the file becomes full.

Related utility: AUDITCON in *Utilities Reference* .

Auditing File object

(AFO) A leaf object in the Novell Directory Services data structure used to manage an audit trail's configuration and access rights.

The audit utility (such as AUDITCON) creates the AFO when you enable auditing. The server then checks for access rights each time a user attempts to access the audit trail.

Authentication

A means of verifying that an object sending messages or requests to NDS is authorized to do so.

Authentication guarantees that only the purported sender could have sent a message or request, and that it originated from the workstation where the authentication data was created.

Authentication works with login restrictions and access control rights to provide a secure network.

All a network user sees of authentication is a request for a password during network login. Every subsequent network operation is transparently authenticated using identification information created when the password was entered.

NetWare 4 authentication uses a Public Key Encryption system that is virtually unbreakable. It consists of a private key and a public key. The keys are strings of numbers used in complex mathematical functions.

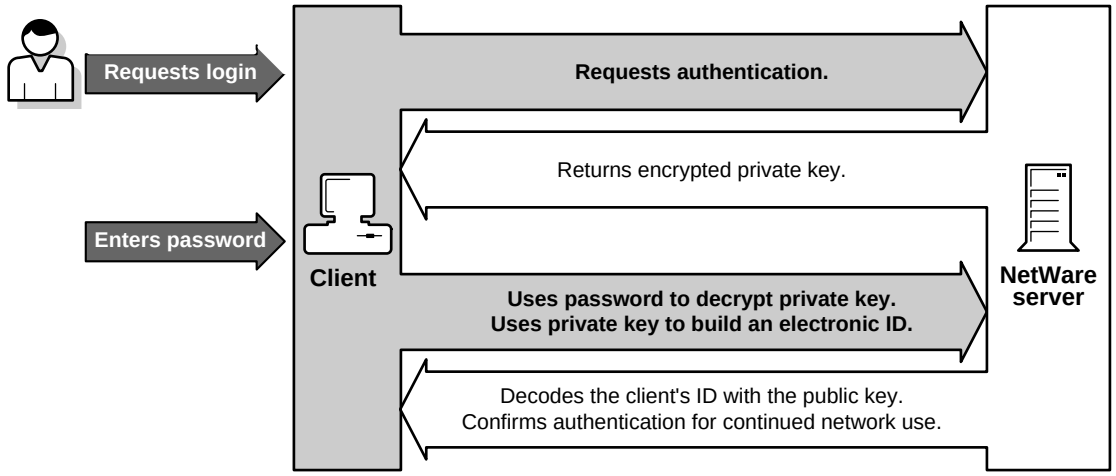
The workstation uses a private key to encode messages sent to the NetWare server. The server then uses a public key to decode the messages. The server

knows that the workstation sent it because the workstation's private key is required to encode the message.

Neither the two keys nor the user's password are ever sent across the network.

Authentication is illustrated in the following figure:

Figure 1-2
Authentication



Because the keys aren't changed during a login session, you might encourage users to log out periodically to update the authentication keys. That way, if someone on the server or workstation got one of the keys, only the current login session would be compromised.

You can force periodic logouts by setting login time restrictions.

AUTOEXEC.BAT

A batch file that executes automatically when DOS is booted on a computer.

A workstation's AUTOEXEC.BAT file, located on the bootable floppy or hard disk, can contain commands that

- Load Novell Client files
- Load other files required by the hardware
- Set the DOS prompt

- Change the default drive to the first network drive
- Log in the user

The workstation AUTOEXEC.BAT file can also load user-specific programs such as NETBIOS.COM or call other batch files.

AUTOEXEC.NCF

A NetWare server executable batch file, located on the NetWare partition of the server's hard disk.

AUTOEXEC.NCF is used to

- Load modules
- Set the NetWare operating system configuration
- Set bindery contexts
- Store the IPX™ internal network number
- Store the file server name
- Make time zone settings

The network supervisor can also add executable server commands (such as LOAD INSTALL or LOAD MONITOR) to AUTOEXEC.NCF.

If you choose only the IPX protocol during installation, the AUTOEXEC.NCF contains all LOAD and BIND commands for the LAN drivers, network boards, and for the IPX protocol.

In addition, if you enable your server for non-routing TCP/IP, the LOAD and BIND commands are placed in the AUTOEXEC.NCF file.

See also “NETINFO.CFG” ; “Router.”

Automatic rollback

A feature of TTS that returns a database to its original state.

When a network running under TTS fails during a transaction, the database returns, or rolls back, to its most recent complete state, preventing corruption from an incomplete transaction.

See also “Transaction Tracking System.”

Autonomous system

A collection of routers and networks under a single administrative control.

See also “Exterior Gateway Protocol.”

Chapter

2 *B*

Backup

A duplicate of data (file, directory, volume), copied to a storage device (floppy diskette, cartridge tape, hard disk). A backup can be retrieved and restored if the original is corrupted or destroyed.

The type of backup you perform and the storage media rotation method you use are dictated by

- The number of backup sessions you are willing to restore in the event of data loss
- The number of duplicate copies of data you want and are willing to store
- The maximum age you want the oldest data copy to be

Perform backups when the fewest files are likely to be open. (Files in use at the time of the backup aren't backed up.)

How Often to Back Up Files

Files that don't change often, such as applications or archived files, don't need to be backed up as frequently as files that change often.

In deciding which files to back up and how often to back them up, imagine a worst case scenario: Determine how long it would take and what it would cost to re-create critical information if an unexpected failure caused data loss at the worst possible time.

How File Restoration Decisions Determine Backup Methods

Backup methods have different implications for the process of restoring files. Before you decide which backup method works best, make sure you understand the implications.

Amount of Media Required

After you decide what kind of backups you want to perform, determine how many sets of storage media you need, and how you plan to rotate them.

Rotation Methods

Rotation distributes both current and older data across several storage media, thereby reducing the risk of all data being lost if one of the media becomes corrupted.

Example: The Grandfather Rotation Method

To use the Grandfather rotation method, you need 20 sets of storage media.

Label four as daily sets Monday, Tuesday, Wednesday, and Thursday. Label four as weekly sets Friday1, Friday2, Friday3, and Friday4. Label the other twelve as monthly sets January, February, etc.

Note

You may want to add another set of weekly tapes, labeled Friday5, for months in which there are five Fridays.

The Grandfather method of rotation is illustrated in the following table:

Table 2-1

Daily	Daily	Daily	Daily	Weekly	Monthly
Mon.	Tue.	Wed.	Thu.	Fri. 1	
Mon.	Tue.	Wed.	Thu.	Fri. 2	
Mon.	Tue.	Wed.	Thu.	Fri. 3	
Mon.	Tue.	Wed.	Thu.	Fri. 4	
					Jan.
Mon.	Tue.	Wed.	Thu.	Fri. 1	
Mon.	Tue.	Wed.	Thu.	Fri. 2	
Mon.	Tue.	Wed.	Thu.	Fri. 3	
Mon.	Tue.	Wed.	Thu.	Fri. 4	
					Feb.

Example: The 10-Tape Rotation Method

To use the 10-tape rotation method, you need ten tape sets, each set labeled with a number from one through ten.

In this method, a 40-week period is divided into 10 four-week cycles, and each tape set is used an equal number of times during the 40 weeks.

You always have a 12-week-old copy of your data on at least one tape set.

For the first four weeks, use the same tape sets for the Monday (set 1), Tuesday (set 2), Wednesday (set 3), and Thursday (set 4) backups.

On the first four Fridays, use the next sequence of four tapes (sets 5 through 8).

During the second four week cycle, increment the daily tape set numbers by one, for example, Monday (set 2), Tuesday (set 3), Wednesday (set 4), and Thursday (set 5).

During the second four weeks, increment the Friday tape set number by one also (sets 6 through 9).

The 10-tape rotation method (showing the tape set numbers) is illustrated in the following table.

Table 2-2

Week 1:	Week 2:	Week 3:	Week 4:
M, T, W, Th, F	M, T, W, Th, F	M, T, W, Th, F	M, T, W, Th, F
1, 2, 3, 4, 5	1, 2, 3, 4, 6	1, 2, 3, 4, 7	1, 2, 3, 4, 8
2, 3, 4, 5, 6	2, 3, 4, 5, 7	2, 3, 4, 5, 8	2, 3, 4, 5, 9
3, 4, 5, 6, 7	3, 4, 5, 6, 8	3, 4, 5, 6, 9	3, 4, 5, 6, 10
4, 5, 6, 7, 8	4, 5, 6, 7, 9	4, 5, 6, 7, 10	4, 5, 6, 7, 1
5, 6, 7, 8, 9	5, 6, 7, 8, 10	5, 6, 7, 8, 1	5, 6, 7, 8, 2
6, 7, 8, 9, 10	6, 7, 8, 9, 1	6, 7, 8, 9, 2	6, 7, 8, 9, 3
7, 8, 9, 10, 1	7, 8, 9, 10, 2	7, 8, 9, 10, 3	7, 8, 9, 10, 4
8, 9, 10, 1, 2	8, 9, 10, 1, 3	8, 9, 10, 1, 4	8, 9, 10, 1, 5
9, 10, 1, 2, 3	9, 10, 1, 2, 4	9, 10, 1, 2, 5	9, 10, 1, 2, 6
10, 1, 2, 3, 4	10, 1, 2, 3, 5	10, 1, 2, 3, 6	10, 1, 2, 3, 7

Note

To make sure that you have a four-week-old copy of data at the end of the first four-week cycle, back up to tape set 10 as well as to tape set 1 on Monday of the first week.

Backup Log

Keep a written log of all backups performed. The log serves as a record in case the electronic log and error files are destroyed.

Record the date, backup type, what was backed up, the media set identification name or number, session log path, data path, and the initials of the person performing the backup.

Recording the data path in a log makes it easier to provide this information if you want to restore the session to a different location than it was backed up from.

See also “Data set.”

Backup hosts and targets

A backup host is a NetWare server that has a storage device and a storage device controller attached.

A target is the server, workstation, or database from which you back up data or to which you restore data.

Any server, workstation, or service (such as NDS) on the network can be a target, including the backup host. The target server must contain Target Service Agent files.

See also “Backup” ; “Storage Management Services” ; “Target Service Agent.”

Baud rate

In serial communication, the signal modulation rate, or the speed at which a signal changes.

See also “Serial communication.”

Bindery

A network database, in NetWare versions earlier than NetWare 4, that contains definitions for entities such as users, groups, and workgroups.

In NetWare 4, the bindery has been replaced by the Novell Directory database, under NDS.

Bindery services provides NetWare 4 networks with backward compatibility to NetWare versions that used the bindery. (See also “Bindery services.”)

The following table compares features of bindery- and Directory-based versions of NetWare.

Table 2-3

Feature	Bindery	Directory
Logical Structure	Flat structure	Hierarchical tree
Partitions	None	Distributed database
Replication	None	Partitions replicated
Synchronization	No replicas	Replicas synchronized
Users	Separate account on each server	Global account for network
Groups	Server-by-server	Network-wide
Login	Password per server	Network-wide with authentication
Printing	No friendly map	User-friendly access
Volumes	Server-specific	Global objects
Queues	Local objects only	System-wide objects
Trustees	Server-specific	Global objects

Bindery context

The container object in which bindery services is set.

See also “Bindery services.”

Bindery context path

A path statement that allows bindery context to be set in as many as 16 containers. Use the Bindery Context SET parameter to set bindery contexts. Multiple contexts are separated by semicolons. For example:

SET BINDERY CONTEXT =
 OU=Legal.O=Novell; OU=Sales.O=Novell; OU=Mktg.O=Novell

For more information, see SET in *Utilities Reference* .

In previous versions of NetWare 4, you could only set the bindery context in one container (Organization or Organizational Unit) within the Directory tree. All bindery objects had to be located in that container.

In NetWare 4, a bindery context path allows

- Bindery objects on a NetWare 4 server to be located in multiple containers
- NetWare 3 NLM programs that rely on bindery services to access objects in more than one container

Note

All containers in the bindery context path must be in a read/write replica present on the server.

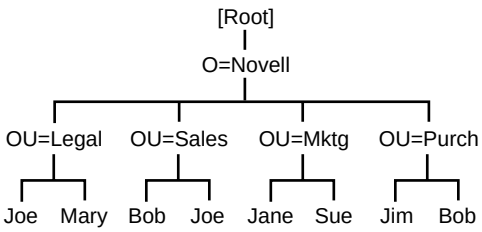
However, using a bindery context path can create a potential problem: Although you cannot have more than one object of the same name in the same container, you can have objects with the same names in the different containers of a bindery context path.

But, you can still have only one object with the same name in a bindery. So, only the object in the first container of a path shows up to users, overriding other objects with the same name in other containers.

It does not matter whether these objects are of the same type (for example, printer Joe and user Joe).

The following illustration shows part of a tree that is included in this bindery context path:

OU=Legal.O=Novell; OU=Sales.O=Novell; OU=Mktg.O=Novell



If the context is specified as shown above, only user Joe in Legal shows up to a user logging in. On the other hand, only user Joe in Sales shows if the user logging in specifies the context as follows:

OU=Sales.O=Novell;OU=Legal.O=Novell;OU=Marketing.O=Novell

Consequently, you should avoid having objects with duplicate names in different containers if these containers are in the same bindery context path.

Related utility: SET in *Utilities Reference* .

See also “Bindery services.”

Bindery object

A leaf object that represents an object placed in the Directory tree by an upgrade or migration utility, but that NDS can't identify.

This object is for backward compatibility with bindery-oriented utilities.

See also “Object.”

Bindery Queue object

A leaf object that represents a queue placed in the Directory tree by an upgrade or migration utility, but that NDS can't identify.

This object is for backward compatibility with bindery-oriented utilities.

See also “Object.”

Bindery services

A feature of NetWare 4 that allows bindery utilities and clients to co-exist with NDS on the network.

Objects in a bindery exist in a flat database instead of a hierarchical database like a Directory tree.

Bindery services creates a flat structure for the objects within an Organization object or within an Organizational Unit object.

All objects within that container object can then be accessed both by NDS objects and by bindery clients and servers. Bindery services applies only to the leaf objects in that Organizational Unit.

The container object where bindery services is set is called the *bindery context* . You can change the bindery context by using the SET command. You can also set multiple bindery contexts. You can have up to 16 bindery contexts for each server. (See Maintaining Bindery Services in a NetWare 4 Environment in *Guide to NetWare 4 Networks* .)

When you install any NetWare 4 server into the Directory tree, a NetWare Server object is created in the container object. By default, bindery services is activated and the bindery context is set for that container object.

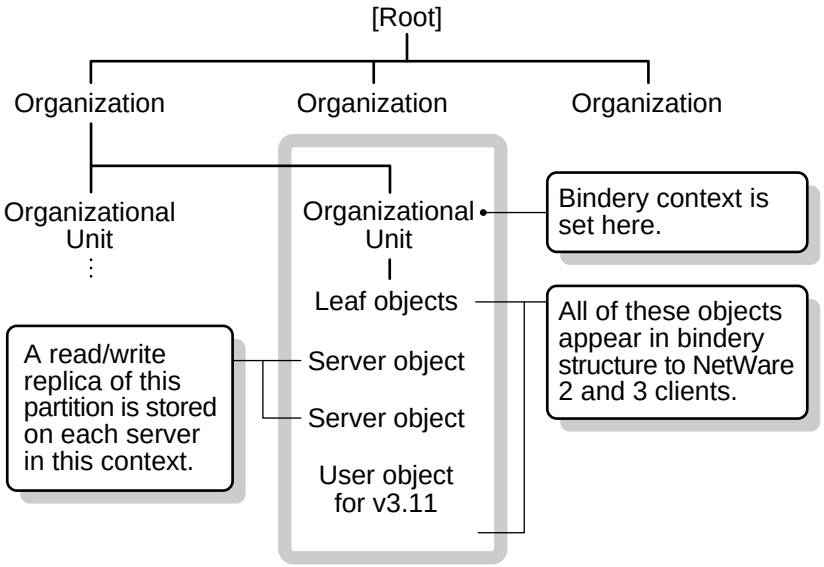
A read/write replica of the Directory partition that the bindery context is located in must be stored on each server you want bindery services enabled on. This is done by default when you install a server into a new context.

If you don't create a new context when installing NetWare 4 on a server (that is, if you place the server object into an existing context), then the installation program places on the server a read/write replica of the Directory partition containing that context.

Although bindery services is enabled during installation of NetWare 4, you can disable it with the SET command.

The following figure illustrates bindery services when a bindery context is set for an Organizational Unit object.

Figure 2-1
Bindery Services in a Directory Tree



If you use NDS Manager to change the default Directory partitions, you must also change the Directory replicas stored on the servers in the bindery context.

The objects in the container object set as the bindery context must have bindery-compatible names. For example, the complete name for a User object might be

MRICHARD.ACCOUNTING.NOVELL US

However, only the common name of the User object can be seen by bindery clients and servers using bindery services. Therefore, the object's common name must match bindery naming rules.

See also "Context" ; "Directory tree" ; "Object" ; Managing the Novell Directory Tree in *Supervising the Network* .

Binding and unbinding

The process of assigning a communication protocol to network boards and LAN drivers and the process of removing it.

Each board must have at least one communication protocol bound to the LAN driver for that board. Without a communication protocol, the LAN driver can't process packets.

You can bind more than one protocol to the same LAN driver and board. You can also bind the same protocol stack to multiple LAN drivers on the server.

You can also cable workstations with different protocols to the same cabling scheme.

Binding communication protocols to boards and drivers

To bind communication protocols to boards and drivers, use the INETCFG program or the BIND console command. Use BIND for each board in the server.

Until a protocol is bound to a board, users attached to the cabling scheme from the board can't log in.

When you bind a protocol to a board, you specify the cabling scheme's IPX external network number.

This hexadecimal number must be the same for all boards cabled together that use the same frame type. The IPX external number must be different from the number used by boards of other frame types and must be different from the addresses of other cabling systems on the network.

The cabling scheme's IPX external network number must also be different from the *internal* network address for any node on the network.

Related utility: BIND in *Utilities Reference* .

See also "IPX external network number."

Unbinding Communication Protocols from Boards and Drivers

To remove a communication protocol from a board and driver, you can use the UNBIND console command or delete the binding in INETCFG. If you have loaded the driver more than once, select the specific board you want to unbind.

Use UNBIND to unbind each board. When the protocol is unbound, users attached to the cabling scheme of the board can't log in.

If users are already logged in, they receive a message when they attempt to access the server.

Related utility: UNBIND in *Utilities Reference* .

See also “Communication protocols” ; “IPX external network number.”

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

The smallest amount of disk space that can be allocated at one time on a NetWare volume.

To minimize RAM requirements in NetWare 4, the block size depends on the size of the volume, as shown in the following table:

Volume size	Block size
0 to 32 MB	4 KB
32 to 150 MB	8 KB
150 to 500 MB	16 KB
500 to 2,000 MB	32 KB
2,000+ MB	64 KB

The block size is set automatically during installation; we recommend that you don't change the default block size.

Block suballocation can subdivide a disk block among several files to make better use of disk space when a large block size is used.

See also “Block suballocation.”

Block suballocation

Allows parts of several files to share one disk block, better utilizing disk space.

Block suballocation divides any partially used disk block into 512-byte suballocation blocks. These suballocation blocks are used to share the remainder on the block with leftover fragments of other files.

Example: Your default block size is 64 KB, and you create a 65KB file.

- Without block suballocation, the 65KB file requires two disk blocks, or 128 KB.
- With block suballocation, you use one disk block (64 KB) plus two 512-byte suballocation blocks. The remaining 63 KB of the second block can still be used by other files.

Block suballocation is set by default when NetWare 4 is installed.

See also “Block” ; “Volume.”

Boot files

Files, like AUTOEXEC.NCF and CONFIG.SYS, that

- Start the operating system and its drivers
- Set environment variables
- Load NetWare

NetWare server boot files include

- **AUTOEXEC.NCF** loads modules and sets the NetWare operating system configuration. (See also “AUTOEXEC.NCF.”)
- **STARTUP.NCF** loads the servers' disk driver and some SET parameters.

Workstation boot files depend on the client type (DOS, Windows, and UNIX®). See your client manual.

BOOTCONF.SYS

A file used by a workstation using Remote Reset to determine which remote boot image file to use.

See also “Remote printer mode.”

BOOTP

A protocol used by some hosts to obtain their IP address.

The host broadcasts a BOOTP request on the local network. If the server is attached to the same network as the host, it receives the request and replies with a packet that contains the host's address.

If the server is on a different network, a BOOTP forwarder must direct the broadcast to a BOOTP server and forward the reply to the host.

The TCP/IP software provides BOOTPFWD.NLM, which enables your machine to forward BOOTP request and reply packets between the BOOTP server and BOOTP clients.

BOOTP forwarding with NetWare can be configured for use with up to four different BOOTP servers.

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 topologies and determines the most efficient path.

See also “Router.”

Browse right

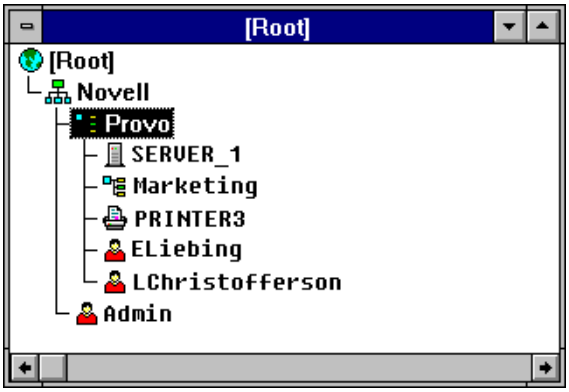
An object right that grants the right to see an object in the Directory tree.

See also “Rights.”

Browsing

A way of finding objects in the Directory.

Objects in the Directory are in hierarchical order. Since the Directory can be very large, you can browse the tree structure to find the object you need.



Example: To find object PRINTER3 when you aren't sure where it is, look at objects in your current context.

If PRINTER3 isn't in your current context, search up or down the Directory tree until you find it, or use the browser's search feature.

Related utilities: NETADMIN and NetWare Administrator in *Utilities Reference*.

Btrieve

A complete key-indexed record management system designed for high-performance data handling.

The Btrieve* program stores information in Btrieve data files. Numerous existing database programs recognize the Btrieve data file format, and you can use Btrieve with any of these database programs.

Btrieve supports concurrent access; more than one user or application can access a Btrieve data file at the same time.

Btrieve maintains the data file's integrity during concurrent access. That is, Btrieve ensures that the information in the data file isn't corrupted.

The Btrieve Record Manager can run on a NetWare server, called *server-based* Btrieve, or on a workstation, called *client-based* Btrieve.

Server-Based Btrieve

This product is packaged with the NetWare operating system and comes as a series of NLM files for the NetWare server.

Server-based Btrieve also includes a collection of other executable files for workstations that need access to Btrieve data files on that server (or on any other NetWare server running server-based Btrieve).

Using these NLM files and executable files, you can run both Btrieve applications that reside on the NetWare server and those that reside on a workstation.

Client-Based Btrieve

This product is available only as part of the Btrieve Developer's Kit (purchased separately from the NetWare operating system). The kit provides developers with a set of tools to create new Btrieve applications.

The Btrieve Developer's Kit consists of the client-based Btrieve Record Manager, an application programming interface (API) to give your application access to the information in Btrieve data files and to documentation for the API.

Client-based Btrieve can run under several operating systems, including DOS and Windows.

Client-based Btrieve allows you to run Btrieve applications that reside on your local workstation and to access Btrieve data files that reside on a NetWare server.

See *Btrieve Installation and Operation*.

Buffer

An area in server or workstation memory set aside to temporarily hold data, such as packets received from the network.

See “Cache buffer” ; “Packet receive buffer.”

Chapter 3 C

Cache buffer

A block of NetWare server memory (RAM) in which files are temporarily stored. Cache buffers greatly increase NetWare server performance.

The cache buffer size depends on the default block size, which depends on the size of the volume. (See “Block.”)

Cache buffers allow workstations to access data more quickly because reading from and writing to memory is much faster than reading from or writing to disk.

See also “Cache buffer pool.”

Cache buffer pool

The amount of memory available for use by the operating system after the SERVER.EXE file has been loaded into memory.

The operating system uses cache buffers in a variety of ways:

- To cache a volume's File Allocation Table (FAT) and suballocation tables in memory
- To cache parts of a volume's Directory Entry Table (DET)
- To cache parts of files for users to access
- To build a hash table for directory names
- To build Turbo FAT indexes for open files that are randomly accessed and have 64 or more regular FAT entries

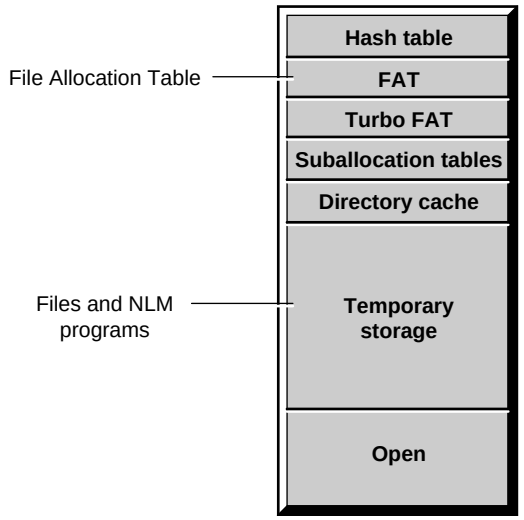
- To use with NLM programs such as LAN drivers, disk drivers, INSTALL (used to create and modify NetWare partitions and volumes), VREPAIR (used to repair NetWare server tables), database servers, communications servers, and print servers

  When an NLM is removed from server memory, the NLM returns the borrowed memory to the cache buffer pool.

Cache memory

Available RAM that NetWare uses to improve NetWare server access time.

Cache memory allocates memory for the hash table, the FAT, the Turbo FAT, suballocation tables, the directory cache, a temporary data storage area for files and NLM files, and available memory for other functions.



If the cache memory uses the default block size and a file takes more than one block, the file is placed in a second noncontiguous block both in cache memory and on the volume (on the hard disks). (See “Block.”)

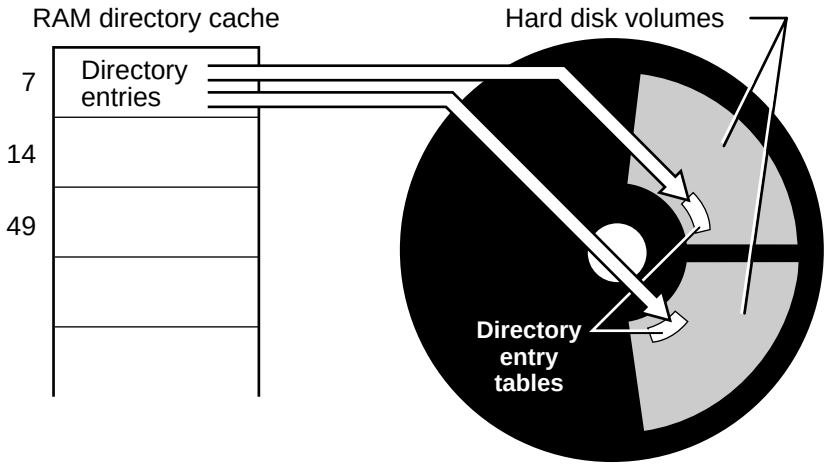
Directory Caching

A method of decreasing the time it takes to determine a file's location on a disk.

The FAT and DET are written into the server's memory. The area holding directory entries is called the *directory cache* .

The server can find a file's address from the directory cache much faster than retrieving the information from disk.

Figure 3-1
Directory Caching

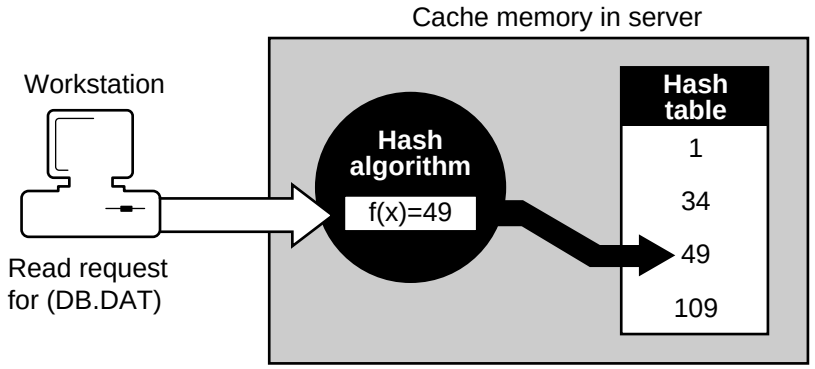


File Caching

A server can service requests from workstations up to 100 times faster when it reads from and writes to the server's cache memory, rather than reading from or writing to the server's hard disks.

The following figure illustrates how a workstation makes a read request from the server and how the server executes a hash algorithm to calculate the file's address from a hash table.

Figure 3-2
File Caching

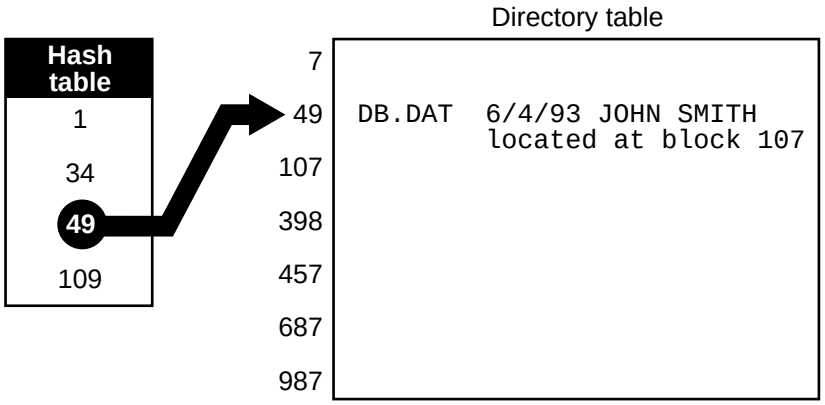


Hashing is a quick way of predicting the file's address in the directory table.

For example, the address on the hash table contains pointers to the first and second probable locations of the DB.DAT file's directory entry in the directory cache.

If the first search isn't successful, the server uses the second pointer to find the directory entry, as illustrated in the following figure:

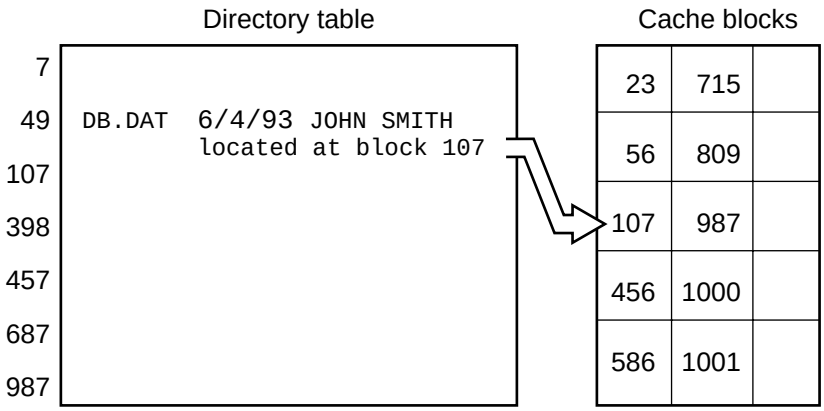
Figure 3-3
Locating the Directory Entry



When the directory entry is located, the server first checks its cache memory to see if it has a copy of DB.DAT.

Figure 3-4

Locating the File in the Cache Memory



If the file is there, the server sends the file to the station from memory. If the file isn't there, the server retrieves the file from disk and sends it to the station.

Writing Files to Cache

When a workstation writes a file to the server, the server performs the hash algorithm to find the file's cache buffer.

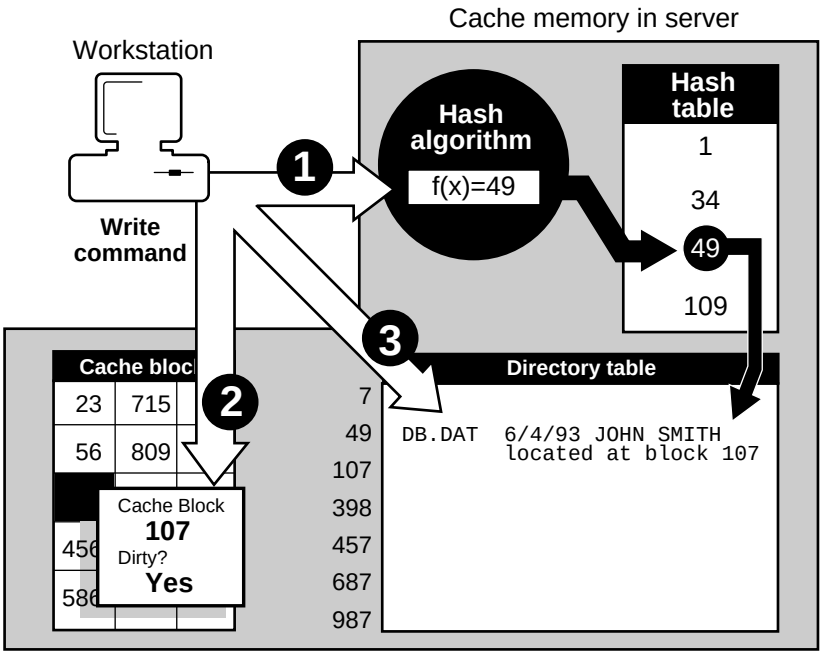
It writes the file to the designated location (writing over the old file, if the file was already in cache) and updates the directory table in the directory cache.

Since the file has changed, its cache buffer is different from the file on disk. The buffer is then referred to as a *dirty cache buffer* .

Since writes to disk take longer to perform than writes to cache, the server keeps the dirty buffer designation on the file in cache until the disk has received the file.

Writing a file to cache is illustrated in the following figure:

Figure 3-5
Writing a File to Cache



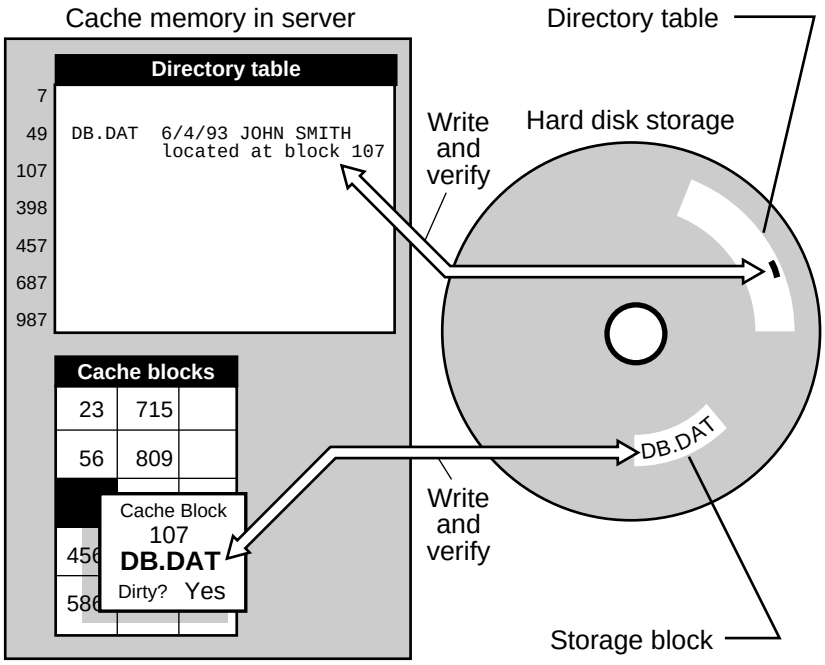
1. Performs hash algorithm
2. Writes file to cache blocks
3. Updates directory table

The server then sends a message to the station that the server has received the file, and the station is free to complete other processes.

Once the file is written to disk, the server checks the data in memory against the data on disk. If there is a match, the buffer is no longer dirty, as illustrated in the following figure:

Figure 3-6

Cache Memory Write and Verify



As the cache memory fills up, buffers containing the least-used files and directories are eliminated.

Related utilities: SERVMAN and SET in *Utilities Reference* .

Can’t Compress (Cc) attribute

A status flag indicating that a file can’t be compressed because of insignificant space savings.

See also “Attributes.”

CDM

(Custom Device Module) The driver component in the NetWare Peripheral ArchitectureTM (NWPA) used to drive specific storage devices attached to the host adapter.

See “NetWare Peripheral Architecture.”

Channel

The path that data flows on to get from the computer to the device. This path can include a host bus adapter, cables, and storage devices.

Character length

In serial communication, the number of bits used to form a character.

See “Serial communication.”

Client

A workstation that uses NetWare software to gain access to the network.

In NetWare, client types include DOS, UNIX, and Windows.

With the respective client software, users can perform networking tasks. These tasks include mapping drives, capturing printer ports, sending messages, accessing files, and changing contexts.

See also “DOS client”; “Workstation.”

Code page

A table storing a character set supporting one or more language scripts. Many personal computers use operating systems that support multiple code pages and allow you to switch between them.

When you press a key on a keyboard (a letter, symbol, or number), the computer receives a numeric code that represents that keystroke. Code pages store these numeric codes.

In a single-byte code page, up to 256 codes are available to represent lower and upper case letters, numbers, punctuation marks, and all the mathematical symbols on your keyboard.

However, 256 codes are not sufficient to represent all the letters and characters used in every language. Some Roman character-based languages, for instance, have a larger alphabet than others and include many accented characters.

For example, a common code page (known as 437) can be used for several Roman character-based languages, including English, French, and German. Portuguese, however, requires a different character set. Code page 860 (Portuguese) removes the symbol for f (franc) and inserts an (O acute).

Other languages such as Chinese, Japanese, and Korean use different characters altogether. The character sets for these languages contain thousands of characters and require a double-byte code page.

The differences between any two single-byte code pages may cause display and readability problems. Differences between single-byte and double-byte code pages usually cause display and readability problems.

Two steps have been taken to help resolve these problems:

- A common code page (850) has been established that handles most character sets of the Roman script.

  This set doesn't include some line drawing characters, and other characters appear in a new location within the table.

- A new convention, called Unicode*, that supports 64,000 characters has been established.

  Unicode provides enough codes to support Roman, Chinese, and other character bases.

Nonetheless, whether you use a common code page or Unicode, any unrecognizable character is substituted in your display. Unrecognizable characters in DOS are displayed as a heart, and in Windows as a box.

Substituted characters can prevent NDS from recognizing an object. For example, you create an Organizational Unit object to represent Finance in western Europe and use code page 852 to make the generic currency symbol a part of its name (OU=¤W-Euro).

When this object is accessed using code page 437, the unsupported currency symbol (¤) is replaced and a new name is sent to NDS. NDS, however, doesn't recognize the new name, and the object can't be opened or accessed—a potentially serious problem.

The only solution is to determine which code page was used to create the object, then view the object using that code page. Determining which code page was used can be time consuming.

See also “Unicode.”

COM ports

Asynchronous serial ports on IBM PC-compatible computers.

See “Serial port.”

Command format

Instructions that show how to type a command at the keyboard, also called *syntax* .

In NetWare manuals, a command format may include constants, variables, and symbols.

Communication

The process of transferring data from one device to another in a computer system.

See also “Network communication” ; “Serial communication.”

Communication buffer

(Formerly used for a *packet receive buffer*) An area in the NetWare server's memory set aside to temporarily hold data packets arriving from workstations.

See also “Packet receive buffer.”

Communication protocols

Conventions or rules used by a program or operating system to communicate between two or more endpoints.

Although many communication protocols are used, they all allow information to be packaged, sent from a source, and delivered to a destination system.

Workstation Protocols

Novell clients may use protocols such as IPX™ , SPX™ , TCP/IP, NetBIOS, OSI, and AppleTalk.

See also “File Transfer Protocol” ; “IPX” ; “SPX.”

Server Protocols

NetWare 4 has six layers of communication between an application and the hardware in the computer. These layers are based on the OSI model.

The six communication layers are

- Application Layer
- Service Protocol Layer
- Communication Protocol Layer
- Link Support Layer
- Driver Layer
- Hardware Layer

In the server, communication protocols allow the Service Protocol Layer to communicate with the Link Support LayerTM (LSL). IPX, part of the operating system, is the default communication protocol.

You can use more than one protocol on the same cabling scheme because the LSLTM, part of the Open Data-Link InterfaceTM (ODI), allows the LAN driver for a network board to service more than one protocol.

Use the following console commands to view, add, and configure communication protocols:

- **PROTOCOL.** Displays the protocols registered with your server and can register others. (See PROTOCOL in *Utilities Reference* .)

- **BIND.** Binds a protocol to a network board installed in the server. (See BIND in *Utilities Reference* .)

- **UNBIND.** Removes protocols from network boards installed in the server. (See UNBIND in *Utilities Reference* .)

The INETCFG utility can also be used to view, add, and configure communication protocols.

See also “Binding and unbinding” ; “Open Data-Link Interface.”

Compare right

A property right that grants the right to compare any other value to a value of that property.

See also “Rights.”

Compressed (Co) attribute

A status flag indicating that a file is compressed.

See also “Attributes.”

Computer object

A leaf object that represents a computer on the network.

In the Computer object's properties, you can store information such as the computer's serial number or the person the computer is assigned to.

See also “Object” ; Creating Leaf Objects in *Supervising the Network* .

Configuration (hardware)

The equipment used on a network (such as servers, workstations, printers, cables, network boards, and routers) and the way the equipment is connected—the network's physical layout.

Hardware configuration includes

- The specific hardware installed in or attached to the computer (such as disk subsystems, network boards, memory boards, and printer boards)
- The set of parameters selected for a board

  For many boards, these settings are made with jumper and switch settings; for other boards, settings are made using configuration software.

Configuration (router)

The settings and parameters chosen through internetwork utilities to configure a NetWare 4 server as a router.

Use INETCFG to

- Configure AppleTalk and TCP/IP packet routing across network segments
- Configure IPX/SPX parameters such as network number and frame type
- Load and bind protocols to the server's network boards
- Enable the NLSP protocol
- Display the most recent console messages

Use FILTCFG to configure RIP/SAP packet filtering.

Configuration (server)

The settings and parameters chosen through INSTALL.NLM while either installing a new NetWare 4 server, or performing maintenance work on an existing NetWare 4 server.

Server configuration includes

- Loading and binding disk, CD-ROM, and LAN drivers
- Assigning an IPX external network number

- Partitioning the server hard disk as NetWare partitions
- Creating NetWare volumes
- Mounting volumes
- Assigning an IPX internal network number
- Modifying volume segments, names, and block size
- Enabling or disabling file compression, block suballocation, data migration
- Binding the IPX protocol
- Installing Novell Directory Services

Optional configuration parameters include

- Mirroring or duplexing NetWare disk partitions
- Increasing the number of licensed connections
- Binding additional protocols such as TCP/IP and AppleTalk
- Disabling Novell Directory Services
- Installing additional NetWare products
- Creating client diskettes
- Adding or changing a server language
- Installing online documentation
- Modifying the STARTUP.NCF and AUTOEXEC.NCF files

Configuration (software)

The software used on a network for servers, clients, protocols, services, drivers, utilities, etc., provides the means to communicate and operate on network hardware.

Software configuration includes

- The specific software installed or copied to the computer storage media
- Configuration utilities and preference options
- The default setting established in each software module
- The set of .NCF, .CFG, .INI, and system configuration files used as reference files for non-default settings

Connection number

A number assigned to any workstation that attaches to a NetWare server; it may be a different number each time a station attaches.

Connection numbers are also assigned to processes, print servers, and applications that use server connections.

The server's operating system uses connection numbers to control each station's communication with other stations.

Related utility: NLIST in *Utilities Reference* .

Connectivity

The ability to link computer systems (PCs, minicomputers, and mainframes) into a network in order to share resources such as applications and printers.

See also “Internetwork.”

Console

The monitor and keyboard where you view and control NetWare server activity.

See also “Server console.”

Console operator

A user or member of a group who has been delegated rights to manage the NetWare server.

Container login script

Sets a general environment for all users in a container (such as an Organizational Unit). These login scripts execute first.

Maintaining many user login scripts can be time consuming. You want to include as much customizing information as possible in the container login script.

For example, if all users need access to NetWare utilities in the same volume, put the search drive mapping to that volume in a container login script.

See also “Login scripts.”

Container object

An object that can hold, or contain, other objects. For example, an Organizational Unit is a container object because it can contain other objects; it doesn't have to.

Container objects are used as a way to logically organize all other objects in the Directory tree.

See also “Object” ; Creating Container Objects in *Supervising the Network* ; NDS Object Classes and Properties in *Guide to NetWare 4 Networks* .

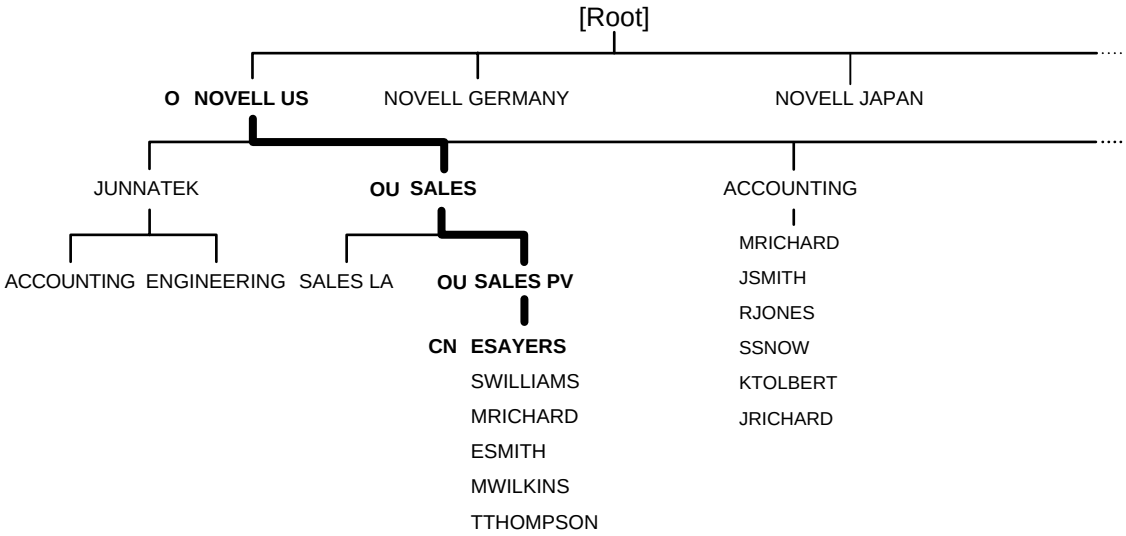
Context

The position of an object within its container in the Directory tree.

NDS allows you to refer to objects according to their positions within a tree. When you add an object (such as a server or user) to the network, you place that object in a container object in the Directory tree.

For example, in the following figure, the context for the User object ESAYERS is SALES PV.SALES.NOVELL US. The context for the User object RJONES is ACCOUNTING.NOVELL US.

Figure 3-7
Context in a Directory Tree



When you move from one container object to another, you *change contexts* . Whenever you change contexts, indicate the complete name of the object you are changing the context to.

If you are referring to an object that is in the same container object as your User object, you need only refer to that object by its common name, instead of by its complete name.

For example, in the previous figure, if the User object ESAYERS located in SALES PV.SALES.NOVELL US wants information on User object ESMITH located in the same context, then ESAYERS need only refer to the User object as ESMITH.

See also “Novell Directory Services” ; “Object” ; “Container object.”

Controller board

A device that enables a computer to communicate with another device, such as a hard disk or tape drive.

The controller board manages input/output and regulates the operation of its associated device.

Controller circuitry is incorporated in most new hard disks and tape drives; a separate controller board isn't used.

Country object

A container object that represents a country where your network resides and organizes other Directory objects with the country.

For example, you could use a Country object for the country where your organization headquarters reside or, if you have a multinational network, for each country that is a part of your network.

Note

The Country object isn't part of the default NetWare 4 server installation. To use a Country object, create it at installation. Using a Country object in NDS isn't a requirement for interoperability with other X.500-compliant directory services.

See also "Object" ; "Container object" ; Creating Container Objects in *Supervising the Network* ; NDS Object Classes and Properties in *Guide to NetWare 4 Networks* .

Create right

A file system right that grants the right to create new files or subdirectories, or to salvage a file after it has been deleted.

Also, an object right that grants the right to create a new object in the Directory tree.

See also "Rights."

Custom Device Module

(CDM) The driver component in NWPATM used to drive specific storage devices attached to the host adapter.

See also "NetWare Peripheral Architecture."

Chapter 4 *D*

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 migration

The transfer of inactive data from a NetWare volume to an optical disc storage device.

Data migration lets you move data to an optical disc storage device, called a *jukebox*, while NetWare still sees the data as residing on the volume.

This frees valuable hard space for often-used files while still allowing slower access to infrequently used files.

For example, a law firm might store case reports on a 500-megabyte (MB) volume with data migration. The firm doesn't want to archive these files because it might need any of them at any time. Any single file, however, has only a small chance of being used.

Data migration allows this firm to transfer all these files from its 500MB hard disk to another storage media. These files no longer reside on the NetWare volume (thus freeing disk space), but take only a few extra seconds to call up.

Data migration is enabled and disabled at the volume level using INSTALL.NLM. You can use file system attributes to mark files as eligible or ineligible for migration.

See also “Attributes” ; “High Capacity Storage System.”

Data protection

A means of ensuring that data on the network is safe.

NetWare protects data primarily by maintaining duplicate file directories and by redirecting data from bad blocks to reliable blocks on the NetWare server's hard disk.

Protecting Data Location Information

A hard disk's DET and FAT contain address information that tells the operating system where data can be stored or retrieved.

If the blocks containing these tables are damaged, some or all of the data may be irretrievable.

NetWare greatly reduces the possibility of losing this information by maintaining duplicate copies of the DET and FAT on separate areas of the hard disk.

If one of the blocks in the original tables is damaged, the operating system switches to the duplicate tables to get the location data it needs.

The faulty sector is then listed in the disk's bad block table, and the data it contained is stored elsewhere on the disk.

Every time the server is turned on, the operating system performs a consistency check on both sets of DETs and FATs to verify that the two copies are identical.

If both sets don't match, a warning is sent, and the network supervisor should run VREPAIR.

Protecting Data against Surface Defects

NetWare hard disks store data in 4, 8, 16, 32, or 64KB blocks. These blocks are specific data storage locations on the disk's magnetic surface. (Block size is the same on all segments of a volume. See also Block.)

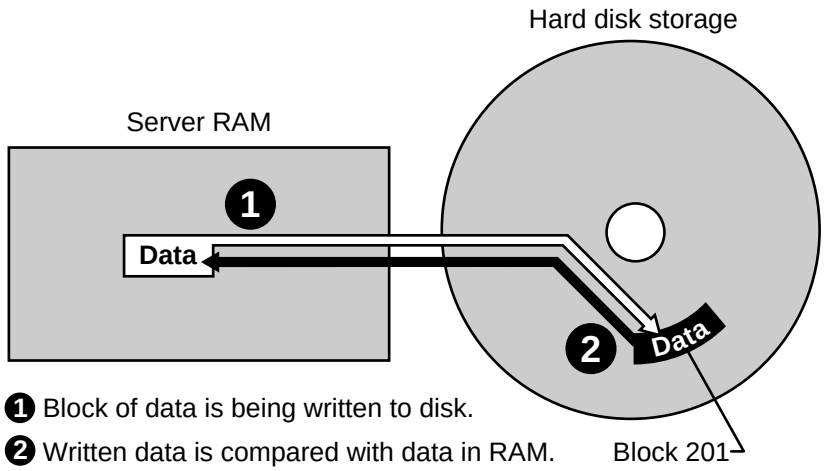
Due to the constant reading and writing of data to disk, some storage blocks lose their capacity to store data.

NetWare prevents data from being written to unreliable blocks by employing two complementary features known as read-after-write verification and Hot Fix™ .

These features, illustrated in the next two figures, enable a hard disk to maintain the same data integrity it had when it was first tested and installed.

Read-after-write Verification. When data is written to disk, the data is immediately read back from the disk and compared to the original data still in memory.

Figure 4-1
Read-after-Write Verification



If the data on the disk matches the data in memory, the write operation is considered successful, the data in memory is released, and the next disk I/O operation takes place.

If the data on the disk doesn't match the data in memory, the operating system determines (after making appropriate retries) that the disk storage block is defective.

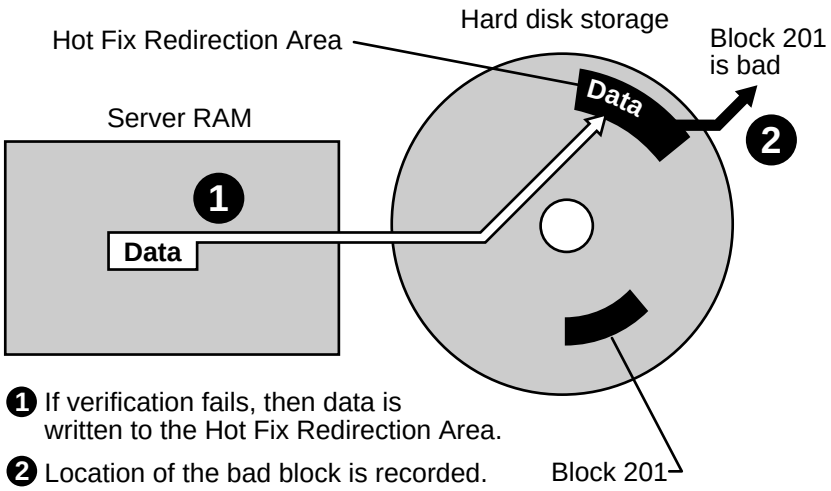
The Hot Fix feature redirects the original block of data (still in memory) to the Hot Fix Redirection Area, where the data can be stored correctly.

Hot Fix Redirection Area. A small portion of the disk's storage space is set aside as the Hot Fix Redirection Area. This area holds data blocks that are redirected there from faulty blocks on the disk.

Hot Fix is always active unless the disk fails and is inoperative, or the redirection area is full.

Once the operating system records the address of the defective block in a section of the Hot Fix area reserved for that purpose, the server won't attempt to store data in the defective block.

Figure 4-2
Hot Fix



Read-after-write verification and Hot Fix are transparent. The network supervisor or a console operator can view Hot Fix activity in SERVMAN or MONITOR.

Disk mirroring or duplexing. You can also protect your data with disk mirroring or duplexing.

Mirroring stores the same data on separate disks on the same controller channel; duplexing stores the same data on separate disks on separate controller channels.

Duplexing is the preferred method since two channels rarely fail simultaneously.

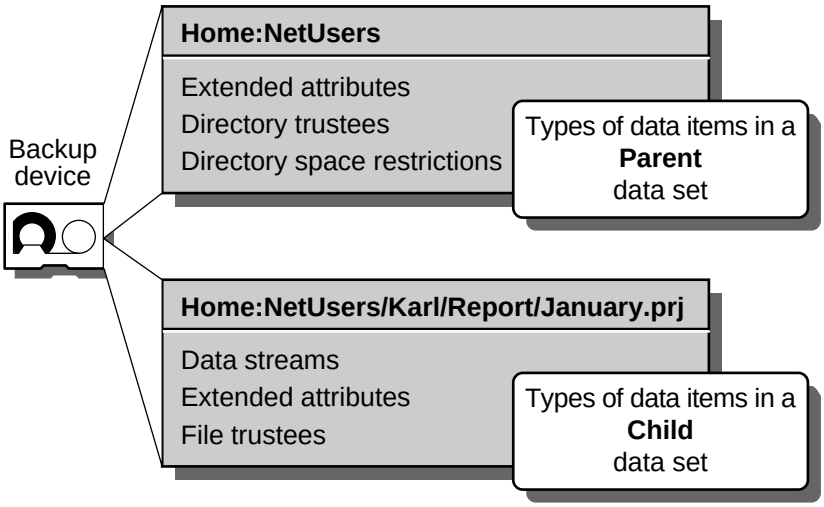
See also “Directory Entry Table” ; “Disk mirroring” ; “Disk duplexing” ; “System Fault Tolerance.”

Data set

A set of data that can be manipulated by SBACKUP.

Data sets can contain different items depending on which Target Service Agent they are related to. The following figure shows typical NetWare data sets.

Figure 4-3
Types of Informational Items Data Sets Contain



See also “Restore.”

Default drive

The drive a workstation is currently using. The drive prompt, such as A:> or F:>, identifies the drive.

Default server

The server you attach to when you load the NetWare Requester™. The default server is the preferred server specified in your NET.CFG file.

Delete Inhibit (Di) attribute

A file system attribute that prevents any user from erasing the directory or file.

See also “Attributes.”

Delete right

An object right that grants the right to delete an object from the Directory tree.

See also “Rights.”

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 **NCOPY F:*.* G:** , the blank space between F:*.* and G: is a delimiter that marks two distinct parameters.

Other delimiters used in NetWare include the comma (,), the period (.), the slash (/), the backslash (\), the hyphen (–), and the colon (:).

Destination server

The NetWare 4 server to which you migrate data files, bindery files, and other information from a previous NetWare version or another network operating system when upgrading to NetWare 4.

See also “Source server.”

DET

(Directory Entry Table) A table that contains basic information about files, directories, directory trustees, or other entities on the volume.

See “Directory Entry Table.”

Device driver

A program (usually an NLM) that controls devices attached to the computer, such as a printer, network board, diskette drive, hard disk, or monitor.

Device drivers expand an operating system's ability to work with peripherals because they control the software routines that make peripherals work.

Device drivers that enable communication between peripherals and the NetWare operating system are NLM programs. Two types of device drivers are disk drivers and NWPA drivers.

Disk Drivers

The disk driver talks to an adapter that is connected by an internal cable to the disk drives.

Depending on the type of disk controller or adapter, one or more disk drives can be connected. Drivers can be loaded into the operating system during installation or at the command line.

Related utility: LOAD in *Utilities Reference* .

NWPA Drivers

The NWPA drivers are called Host Adapter Modules (HAMs) and CDMs, which together help the Media Manager in NetWare keep track of and communicate with a variety of storage devices and media.

Just as disk drivers support adapters and the hard disk devices attached to them, HAMs and CDMs support host adapters and the storage devices attached to them. (HAMs drive the host adapter and CDMs drive the storage devices attached to the host adapter.)

See also “LAN driver” ; “NetWare Peripheral Architecture.”

Device numbering

A method of identifying a device, such as a hard disk, to allow the device to work on the network.

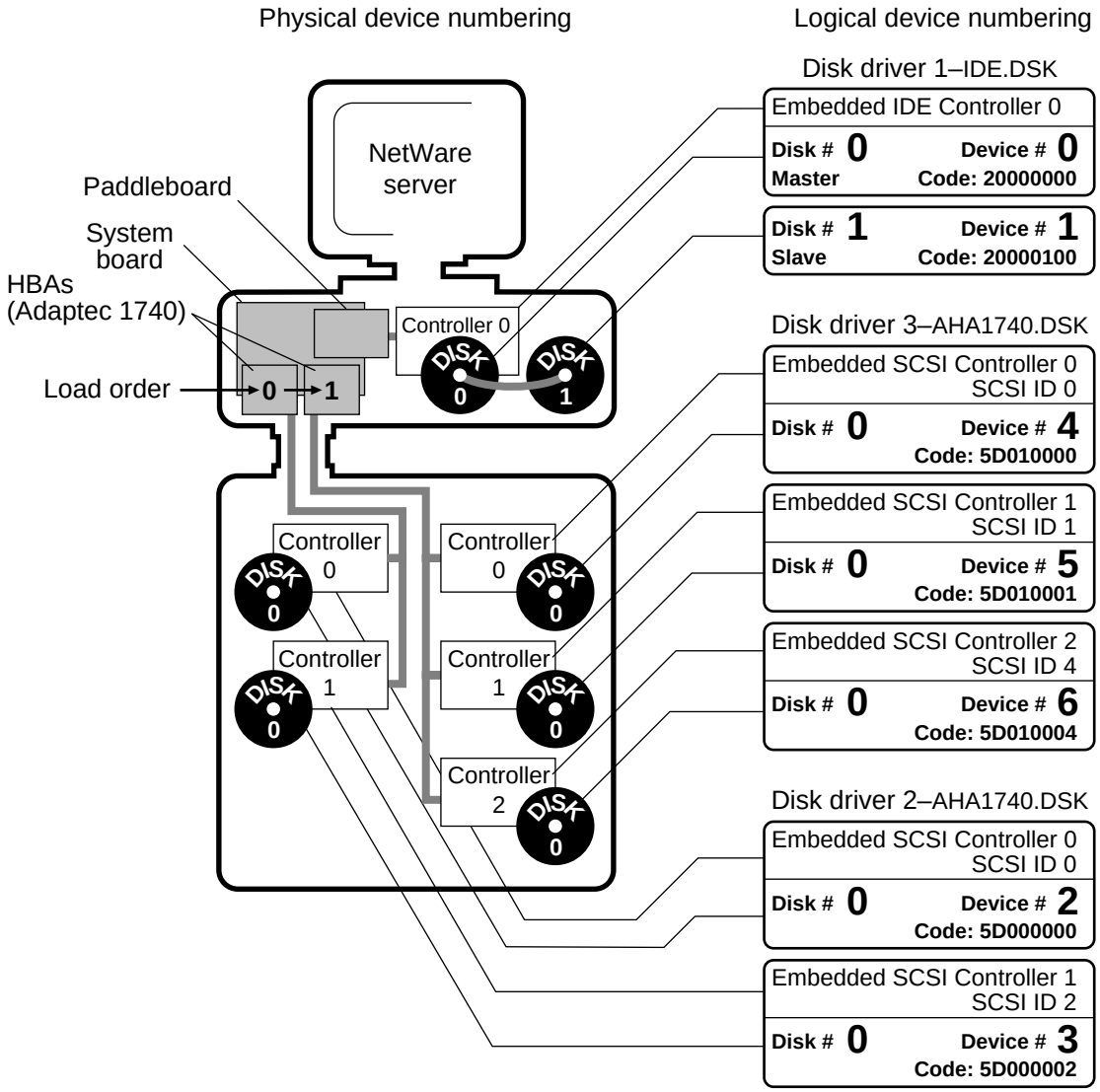
Devices are identified by three sets of numbers:

- Physical address
- Device code
- Logical device number.

The following figure shows how physical addresses correspond to logical numbers and device codes (based on the physical order in which the devices are loaded). Each box in the second column describes the physical address and device code. *Device #* indicates the logical number of the disk.

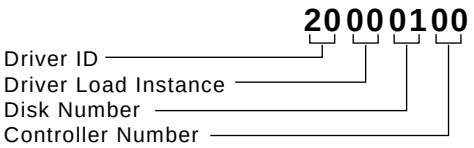
Figure 4-4

Physical and Logical Device Numbering



- **Physical address** is established when the driver reads the address as it was set by jumpers or by software configuration programs.

- **Device code** is determined by the driver ID, driver load instance, disk number, and controller number, as illustrated in the following figure:



- **Logical device number** is determined by the order in which the disk drivers are loaded.

  Both the device code and the logical device number are assigned when the disk driver is loaded. Thus, you must load disk drivers in the same order to maintain the same identification numbers.

  If a disk driver is unloaded and then reloaded, the third and forth digits in the identification number change.

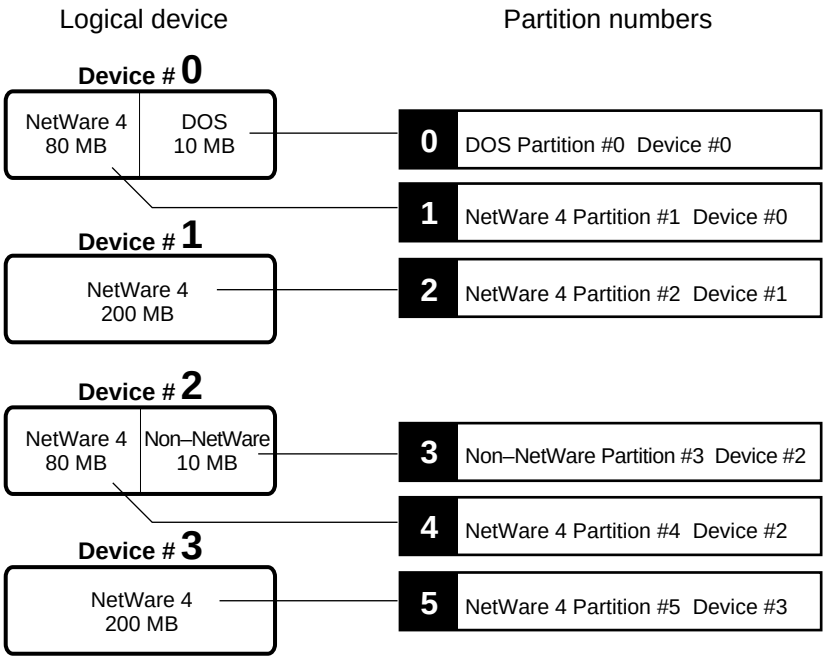
Consider making a chart of your setup. List the order that the disk drivers are loaded in the STARTUP.NCF file. Then, if you receive a message stating that device 1 (20000100) has been deactivated due to disk failure, you know which disk has failed.

After device numbers are assigned, NetWare also assigns physical and logical partition numbers to the partitions created on the hard disks.

The following figure displays the relationship between logical devices and physical partition numbers. Each logical device is assigned a partition number for each type of partition.

Figure 4-5

Logical Devices and Partition Numbers



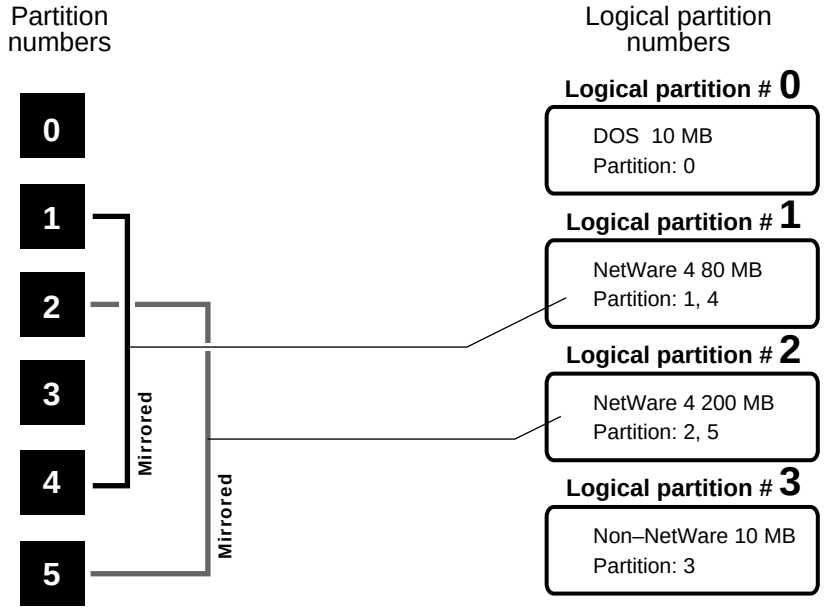
NetWare 4 recognizes boot and NetWare partitions. All other partition types, such as UNIX and partitions, are listed as non-NetWare partitions.

Hot Fix messages use the physical partition number when recording which hard disks have blocks of data that need to be redirected.

All physical partitions are assigned logical partition numbers. These numbers are assigned to both the mirrored disks and the boot and non-NetWare partitions.

The following figure displays the relationship between physical partitions and logical partitions. The chart assumes that partition 1 is mirrored to partition 4 and that partition 2 is mirrored to partition 5.

Figure 4-6
Partition Numbers and Logical Partition Numbers



Mirroring messages use the logical partition number to record which hard disks are being remirrored or unmirrored. (See also “Disk duplexing” ; “Disk mirroring.”)

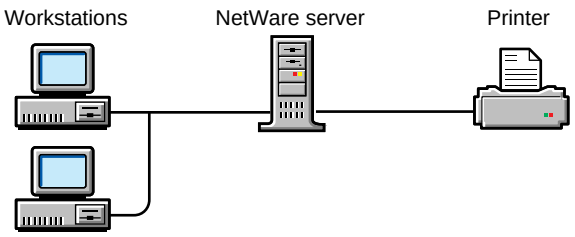
Related utilities: SET and SERVMAN in *Utilities Reference* .

Device sharing

The shared use of centrally located devices (such as printers, modems, and disk storage space) by users or software programs.

By attaching a device to a network that several workstations are logged in to, you can use resources more efficiently.

An example of device sharing is when two clients share disk storage space where Netware volume data is stored. Another example of device sharing is when two network clients have access to a shared printer, as is illustrated in the following figure.



Directory

Directory: A common name for the Novell Directory database, which organizes NDS objects in a hierarchical tree structure called the *Directory tree*. (See “Novell Directory Services.”)

directory: A component in the NetWare file system, used to contain files and subdirectories. (See “File system.”)

Directory and file rights

Rights that control what a trustee can do with a directory or file.

See also “Rights.”

Directory caching

A method of decreasing the time it takes to determine a file's location on a disk.

See also “Cache memory.”

Directory database

A common name for the Novell Directory database.

See also “Novell Directory database.”

Directory entry

Basic information for NetWare server directories and files, such as

- File or directory name
- Owner
- Date and time of the last update (for files)
- Location of the first block of data on the network hard disk

Directory entries are located in a directory table on a network hard disk and contain information about all files on the volume.

The server uses directory entries to track file location, changes made to the file, and other related file properties.

See also “Directory Entry Table.”

Directory Entry Table

(DET) A table that contains basic information about files, directories, directory trustees, or other entities on the volume.

The DET occupies one or more directory blocks on the volume. Each block has 4 KB (4,096 bytes) of data. A directory entry is 128 bytes long, so each block can hold 32 directory entries.

Volume SYS: starts out with seven blocks for its directory table. When a volume needs to add another block to its directory table, the server allocates another block.

The maximum directory blocks per volume is 65,536. Since each block can accommodate 32 entries, the maximum directory table entries per volume is 2,097,152.

The server doesn't cache entire directory tables; it only caches directory blocks in use.

In NetWare 4, a volume can span multiple drives, so each drive can have more than one directory table.

See also “Directory entry.”

Directory Map object

A leaf object that refers to a directory on a volume.

You can't look at the file structure on the volume from the Directory Map object, but login scripts can use the MAP command with a Directory Map object to record the location of frequently used applications.

If the application moves, you need to change only the directory map; all login scripts remain unchanged.

See also “Object” ; Creating and Using Directory Map Objects in *Supervising the Network* .

Directory path

The full specification that includes server name, volume name, and name of each directory leading to the file system directory you need to access.

See also “Drive mapping” ; “File system.”

Directory partition

A common name used for Novell Directory partitions.

See also “Novell Directory partition.”

Directory replica

A common name used for Novell Directory replicas.

See also “Novell Directory replica.”

Directory rights

Rights that control what a trustee can do with a directory.

See also “Rights.”

Directory services

A database built into NetWare 4 that maintains information about every resource on the network.

See also “Novell Directory Services.”

Directory structure

A hierarchical structure that represents how Directory partitions are related to each other in the Directory database. (See also “Directory tree.”)

Also, formerly used to describe the filing system of volumes, directories, and files that the NetWare server uses to organize data on its hard disks. (See also “File system.”)

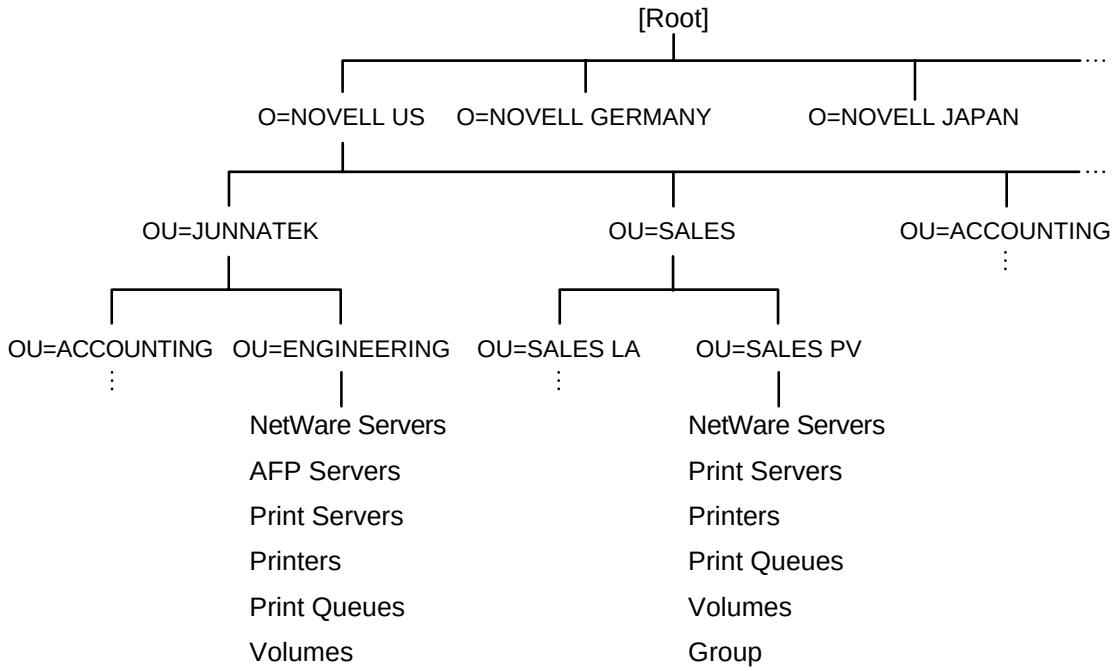
Directory tree

A hierarchical structure of objects in the Directory database. The Directory tree includes container objects that are used to organize the network.

The structure of the Directory tree can be based on a logical organization of objects, and not necessarily on their physical location.

The following figure shows an example of a Directory tree:

Figure 4-7
Directory Tree



See also “Browsing” ; “Object” ; “Novell Directory partition” ; “Novell Directory replica.”

Disk

A magnetically encoded storage medium in the form of a plate (also called a *platter*). The following types of disks are used with personal computers:

- **Hard disk** uses a metallic base and is usually installed within a computer or disk subsystem. (In some cases, they are removable.)
- **Floppy disk** uses a mylar base and is removable.
- **CD-ROM** is a small plastic optical disc that cannot be written to or erased.
- **Optical disc** is either erasable and writable, or WORM (Write Once, Read Many).

See also “Data protection” ; “Disk partition” ; “Hard disk.”

Disk controller

This can be an adapter, board, or a chip set on the mother board. This device controls how data is written to and retrieved from the disk drive.

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.

See also “Host Bus Adapter.”

Disk driver

An NLM that forms the interface between the NetWare operating system and the hard disks. The disk driver talks to an adapter that is connected by an internal cable to the disk drives.

Depending on the type of disk controller or adapter, one or more disk drives can be connected. Drivers can be loaded into the operating system during installation or at the command line.

For specific Novell® driver names and descriptions, see “Device driver.” Other disk drivers are available from third-party vendors.

Related utility: LOAD in *Utilities Reference* .

Disk duplexing

A means of duplicating data to provide data protection. Disk duplexing consists of copying data onto two hard disks, each on a separate disk channel.

This protects data against the failure of a hard disk, or of the hard disk channel between the disk and the NetWare server. (The hard disk channel includes the disk controller and interface cable.)

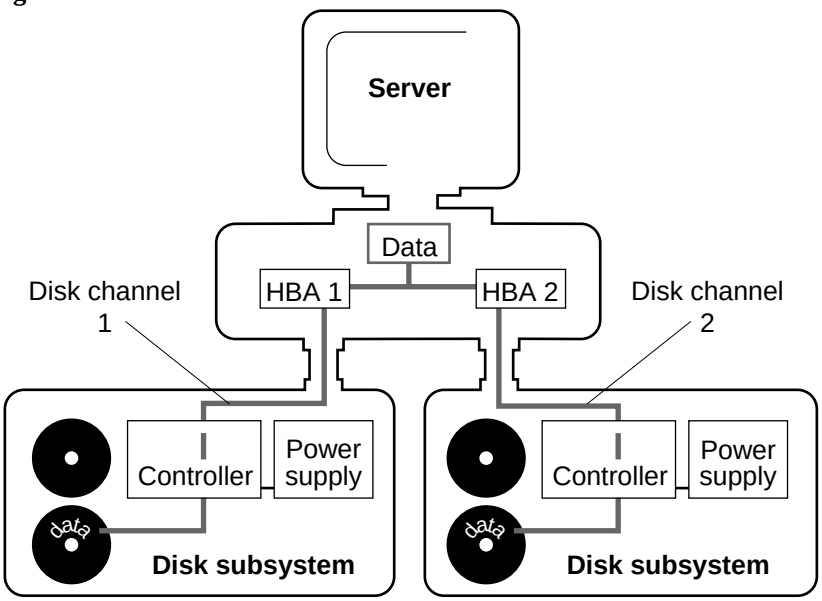
If any component on one channel fails, the other disk can continue to operate without data loss or interruption because it is on a different channel.

The operating system sends a warning message to the console when a drive has failed. Restore the duplexing protection as soon after a failure as possible.

Warning

Because the warning message can scroll off the console screen before you see it, we recommend that you check the status of disk mirroring periodically to ensure that the channels are synchronized.

Figure 4-8
Disk Duplexing



Note

Duplexing alone doesn't guarantee data protection. If both disk channels fail at the same time, or if the computer itself fails, you still lose your data. Therefore, back up your data regularly. Use SBACKUP or another backup utility.

Disk duplexing allows the same data to be written to all disks simultaneously.

Since the disks are on different channels, data transfer is faster than with disk mirroring, where data is written to the disks sequentially over the same channel.

Disk duplexing also allows *split seeks* . This sends read requests to whichever disk can respond first. Multiple read requests are also split between the duplexed disks for simultaneous processing.

Related utility: INSTALL in *Utilities Reference* .

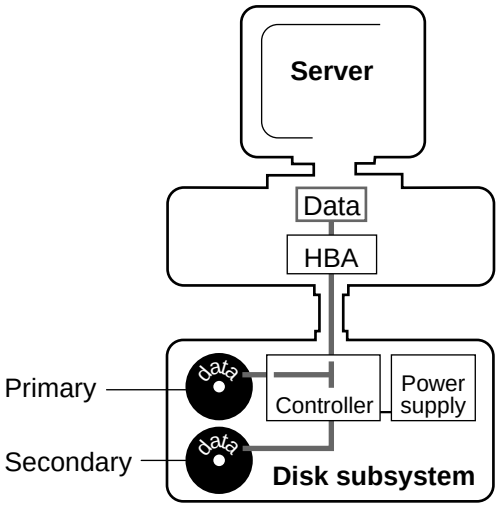
See also “Device numbering” ; “Disk mirroring.”

Disk mirroring

The duplication of data from the NetWare partition on one hard disk to the NetWare partition on another hard disk.

When you mirror disks, two or more hard disks on the *same channel* are paired. Blocks of data written to the original (primary) disk are also written to the duplicate (secondary) disk.

The disks operate in tandem, constantly storing and updating the same files. Should one of the disks fail, the other disk can continue to operate without data loss or interruption.



Note

Mirroring alone doesn't guarantee data protection. If both hard disks fail at the same time, or if the computer itself fails, you still lose your data. Therefore, back up your data regularly. Use SBACKUP or another backup utility.

If one of the disks fails, the operating system sends a warning to the console to indicate the failure so that the mirroring protection can be restored as soon as possible.

Warning

Because the warning message can scroll off the console screen before you see it, we recommend that you check the status of disk mirroring periodically to ensure that the channels are synchronized.

Because disk mirroring duplicates disks on the same channel, it doesn't protect against failures that may occur along the channel between the disks and the NetWare server.

A problem in the channel would cause a failure in both disks.

See also "Device numbering" ; "Disk duplexing."

Disk partition

A logical unit that NetWare server hard disks can be divided into.

In NetWare 4, a NetWare partition is created on each hard disk.

Note

NetWare disk partitions are not related to NDS partitions. Disk partitions are subdivisions of a hard disk. An NDS partition is a subtree within the NDS directory tree. (See also "Partition (disk).")

Volumes are created from the pool of NetWare partitions. A volume consists of one or more volume segments.

One of the server's internal hard disks can contain both an active, primary boot partition, and a NetWare partition.

You need only one boot partition; the other hard disks need to contain only a NetWare partition.

A NetWare partition consists of a Hot Fix Redirection Area plus a large data area. The logical sector 0 of a NetWare partition is the first sector of the data area.

The following figures illustrate how hard disks can be partitioned:

Figure 4-9

Disk Partition: Single Volume

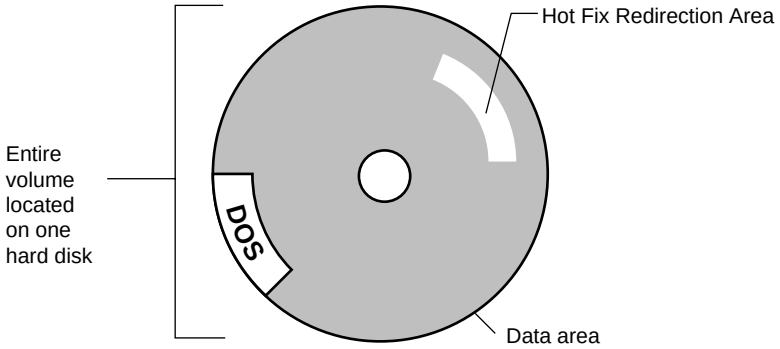
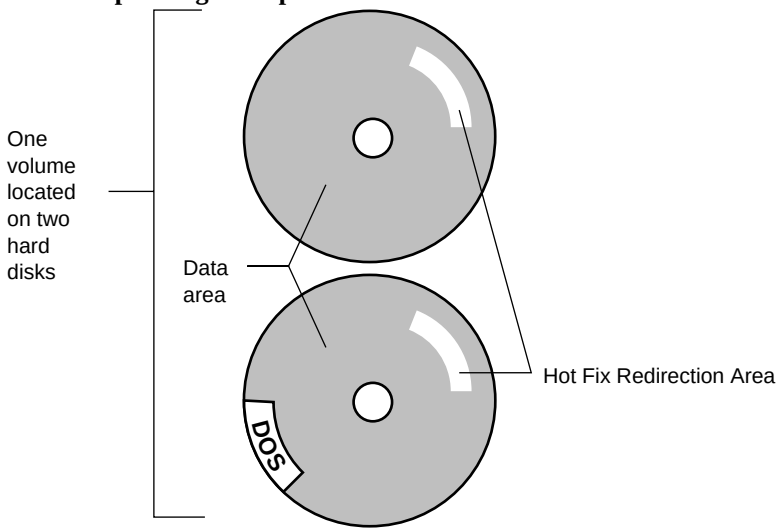


Figure 4-10

Disk Partition: Volume Spanning Multiple Disks



A data area contains four copies of the Volume Definition Table (VDT). Each table contains a list of all volume segments in that NetWare partition.

Four copies are maintained for fault tolerance. If a disk error occurs and one table is corrupted, the error can be detected and corrected.

The rest of the data area can contain one to eight volume segments. Each segment can belong to the same volume or to a different volume.

Related utility: INSTALL in *Utilities Reference* .

See also “Data protection” ; “Hot Fix” ; “Volume.”

Disk space restrictions

Restrictions system administrators can use to set:

- The maximum disk space a user (or other NDSTM object) can use on a particular volume. Users cannot create new files or extend existing files if the users are over their allocated disk space.
- The maximum disk space that can be in a particular directory (and its subdirectories). Directory disk space restrictions are placed on a given directory and limit the amount of disk space that can be used by files in the directory and all its subdirectories.

Both user and directory disk space restrictions can be made in units of either 512 or 4096 bytes.

See also “Owner” ; “Rights.”

Distance vector

An algorithm that disseminates routing information to routers on a network.

A router using the distance vector algorithm maintains only enough information to know how to reach the next router destination (hop) on the network.

Distance vector routers periodically forward this information to each other, even if it has not changed since the last update. Such broadcasts create unnecessary traffic on the network and consume router CPU time.

Distribution List object

A leaf object that represents a list of mail recipients.

For example, you can create a Distribution List object called Recreation Committee. When anyone wants to send a message to all the members in the Recreation Committee, they can simply address their mail to Recreation Committee.

The member of a Distribution List can be a user, another Distribution List object, a Group object, or an Organizational Role object.

Although you can send mail to all the members of a Group, there are some differences between a Distribution List and a Group:

- Members of a group are security equal to the Group object, but the members of a Distribution List are not security equal to the Distribution List.
- A Group is used mainly to simplify assigning trustee assignments and creating login scripts, whereas a Distribution List is used for simplifying sending mail to a list of recipients.
- A Distribution List can have another Distribution List as a member, but a Group cannot have another Group as a member.

Don’t Compress (Dc) attribute

A file system attribute that prevents files from being compressed.

See also “Attributes.”

Don’t Migrate (Dm) attribute

A file system attribute that prevents files from being migrated to a secondary storage device (such as a tape drive or optical disc).

See also “Attributes.”

Don’t Suballocate (Ds) attribute

A file system attribute that prevents an individual file from being suballocated, even if suballocation is enabled for the system.

Use for files that are often enlarged or appended, such as certain database files.

See also “Attributes.”

DOS client

A workstation that boots with DOS and gains access to the network through either

- The requester software (for NetWare 4).
- A NetWare shell (for NetWare 3).

With DOS client software, users can perform networking tasks. These tasks include mapping drives, capturing printer ports, and sending messages. Using the NetWare Requester in NetWare 4, users can change contexts.

See also “Client.”

DOS device

A storage unit compatible with the DOS disk format—usually a disk drive or tape backup unit.

The UPGRADE and SBACKUP utilities both write to a DOS device. The DOS device should be a read/write device.

Because the utilities both read and write data, the media the DOS device uses must allow the data to be updated or changed.

The following devices can be used. If the device runs out of storage space on the media, you are prompted to insert another one.

- Workstation floppy disk drives (can't be used with SBACKUP)
- Tape drives with a DOS device driver
- Optical drives that are read/write devices and have a DOS device driver

The following devices can also be used as DOS devices:

- Workstation hard disk drives
- Network drives
- An optical drive or a WORM drive that has a DOS device driver

DOS Requester

The DOS client software portion of NetWare 4.

See also “NetWare DOS Requester.”

DOS version

The version number and name of the DOS you are using (Novell DOS 7™ , MS DOS* 3.3, etc.).

Different machines use different versions of DOS, which are generally not compatible.

Since all DOS versions have identically named utilities and command interpreters, you can't place the files of different DOS versions in the same directory.

You must create a DOS directory for each workstation type or DOS version you use and load the DOS files into it.

See also “File system” ; “Login scripts.”

Drive

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

Logical drive. An identification for a specific directory located on a disk drive. For example, network drives point to a directory on the network, rather than to a local disk.

Drive mapping

A pointer to a location in the file system, represented as a letter assigned to a directory path on a volume.

To locate a file, you follow a *path* that includes the volume, directory, and any subdirectories leading to the file.

You create drive mappings to follow these paths for you. You assign a letter to the path, and then use the letter in place of the complete path name.

Drive mappings can be temporary or permanent:

- *Temporary mappings.* To map a drive so you can use it during your current session, use the NetWare MAP utility (from a DOS workstation). The mapping is only valid until you log out.

- *Permanent mappings.* To make drive mappings so you can use them every time you log in, place MAP commands in your login script. (See also “Login scripts.”)

NetWare recognizes four types of drive mappings: local drive mappings, network drive mappings, network search drive mappings, and Directory Map objects.

Local Drive Mappings

Local drive mappings are paths to local media such as hard disk drives and floppy disk drives.

In DOS 3.0 and later versions, drives A: through E: are reserved for local mappings.

To change this default, (for example, if you are using the NetWare DOS Requester, you need all of your drives mapped as DOS drives) use the DOS LASTDRIVE command in your workstation CONFIG.SYS file.

Network Drive Mappings

Network drive mappings point to volumes and directories on the network. Normally, drives F: through Z: are used for network mappings. Each user can map drive letters to different directories.

To create a network drive mapping, use the MAP command, the NETUSER text utility, or the NetWare User Tools graphical utility

Network Search Drive Mappings

Network search drive mappings point to directories containing files such as applications or files.

Search drive mappings enable the system to locate a program even if it isn't located in the directory you're working in.

Search drive mappings are numbered, although they also have drive letters. For example, search drive 1 (or S1) may also be known as network drive Z:.

You can map up to 16 network search drives (letters K: through Z:, starting with Z:). You can't map a search drive and a regular network drive to the same letter.

When you request a file and the system can't find it in your current directory, the system looks in every directory a search drive is mapped to.

The system searches, following the numerical order of the search drives, until either the program file is found or can't be located.

Directory Map Objects

Directory Map objects can point to directories that contain frequently-used files such as applications.

If you create a Directory Map object to point to an application, users can access the application by clicking on the Directory Map icon from the browser.

If the application's location in the directory structure changes, you can update the object instead of having to change all users' drive mappings.

Related utilities: MAP and NETUSER in *Utilities Reference* .

Driver

Software that forms the interface between the NetWare operating system and devices such as hard disks or network boards.

See "Device driver" ; "LAN driver."

Dual processing

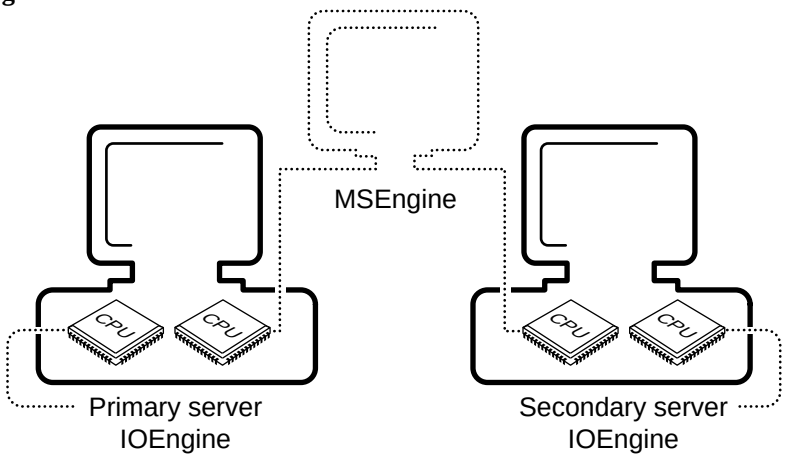
A NetWare® SFT IIITM configuration that assigns parts of the operating system to separate processors.

Because SFT III is split into two engines (the IOEngine and the MSEngine), it is possible to run each engine on a separate CPU, creating a dual processing system.

However, unless such a system is extremely busy, the extra CPU does not help network performance. Dual processing improves performance only when the servers are being utilized at near maximum capacity.

The following figure shows how a dual processing system is configured:

Figure 4-11
Dual Processing



Duplexing

A means of duplicating data to provide data protection. Disk duplexing consists of copying data onto two hard disks, each on a separate disk channel.

See “Disk duplexing.”

Dynamic configuration

A means of allowing the NetWare server to allocate resources according to need and availability.

When the server boots, all free memory is assigned to file caching. As demand increases for other resources (directory cache buffers, for example), the number of available file cache buffers decreases.

The operating system doesn't immediately allocate new resources when a request is received. It waits a specified amount of time to see if existing resources become available to service the demand.

If resources become available, no new resources are allocated. If they don't become available within the time limit, new resources are allocated.

The time limit ensures that sudden, infrequent peaks of server activity don't permanently allocate unneeded resources.

The following parameters are dynamically configured by the operating system:

- Directory cache buffers
- File locks
- Kernel processes
- Kernel semaphores
- Maximum number of open files
- Memory for NLM programs
- Router/server advertising
- Routing buffers
- Service processes
- TTS transactions
- Turbo FAT index tables

Related utilities: MONITOR , SERVMAN , and SET in *Utilities Reference* .

Chapter 5 *E*

Effective rights

The rights that an object can actually exercise to see or modify a particular directory, file, or object.

An object’s effective rights to a directory, file, or object are calculated by NetWare each time that object attempts an action.

Effective rights to a file or directory are determined by

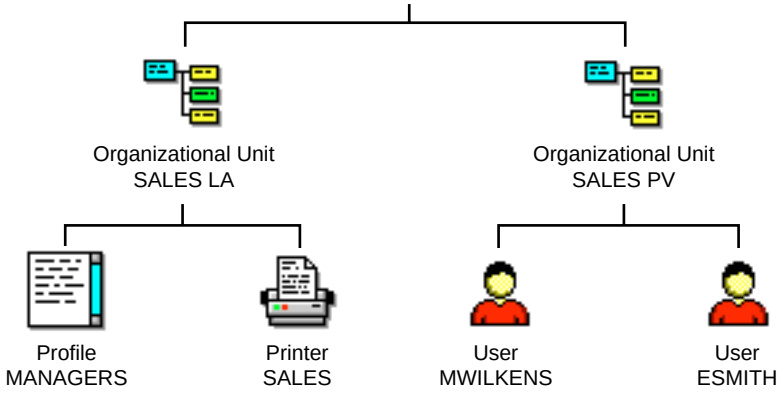
- An object's trustee assignments to the directory, file, or other object
- Inherited rights from an object's trustee assignments to parent directories
- Trustee assignments of Group objects that a User object belongs to
- Trustee assignments of objects listed in a User object's Security Equal To list

If a user has a trustee assignment to a directory on a given level in the directory structure and one on a higher level, the current trustee assignment overrides the one at the higher level.

Trustee assignments to a group, however, are added to individual user trustee assignments.

Effective rights to an object are shown in the following figure:

Figure 5-1
Effective Rights



In the figure, MWILKENS' effective rights to access the MANAGERS profile can come from

- Trustee assignments to MANAGERS that list MWILKENS (rights are explicitly granted)
- Trustee assignments to MANAGERS that list SALES PV (rights are inherited from the trustee's container)
- Trustee assignments to SALES LA that list MWILKENS (rights are inherited from the object's container)

  Rights must pass through MANAGERS' Inherited Rights Filter before becoming effective.
- Trustee assignments to SALES LA that list SALES PV (inherited from object's container and trustee's container)

  Rights must pass through MANAGERS' Inherited Rights Filter before becoming effective.
- Trustee assignments to any Group object that MWILKENS is a member of (rights are only valid when the object requesting rights is a User object)
- Trustee assignments to any object listed in MWILKENS' Security Equal To list (only valid when the object requesting rights is a User object)

If MWILKENS has a trustee assignment to SALES LA and to MANAGERS, the trustee assignment on MANAGERS overrides the trustee assignment on SALES LA.

No rights are granted by default. They must be granted by a trustee assignment at some point.

Related utilities: FILER , NETADMIN , and RIGHTS in *Utilities Reference* .

See also “Inherited Rights Filter” ; “Security” ; “Trustee.”

EGP

(Exterior Gateway Protocol) A protocol that exchanges network reachability information between autonomous systems.

EGP is part of the TCP/IP protocol suite.

See “Exterior Gateway Protocol.”

Elevator seeking

Organizes the way data is read from hard disk storage devices.

A shared network disk drive and its related channel can quickly become clogged with disk I/O requests. Elevator seeking logically organizes disk operations as they arrive at the server for processing.

A queue is maintained for each disk driver operation within the server. As disk read and write requests are queued for a specific drive, the operation system prioritizes incoming requests based on the drive's head position.

As the disk driver services the queue, subsequent requests are located either in the vicinity of the last request or in the opposite direction. Drive heads operate in a sweeping fashion, from the outside to the inside of the disk.

Thus, elevator seeking improves disk channel performance by significantly reducing disk head thrashing (rapid back-and-forth movements) and by minimizing head seek times.

Erase right

A file system right that grants the right to delete directories, subdirectories, or files.

See also “Rights.”

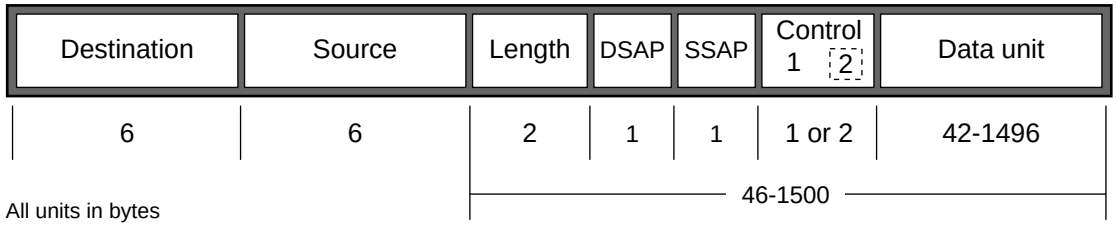
Ethernet configuration

The setup that allows communication using an Ethernet environment.

In an Ethernet environment, stations communicate with each other by sending data in frames along an Ethernet cabling system.

Different Ethernet standards use different frame formats. NetWare 4 uses the IEEE 802.2 standard by default. The following figure illustrates the Ethernet 802.2 frame:

Figure 5-2
Ethernet 802.2 Frame



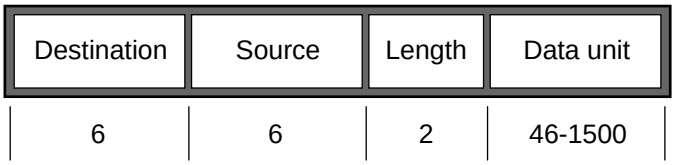
To configure stations for Ethernet standards other than 802.2, use a *frame statement* . For servers and routers, add the frame statement to the LOAD command. For workstations, add the frame statement to the NET.CFG file.

In addition to 802.2, you can use one of the following frame types:

- **Ethernet 802.3** is used as the default in NetWare 3.11 and earlier versions. This frame type is also referred to as the *raw* frame. Don't use this frame on a network that uses protocols other than IPX.

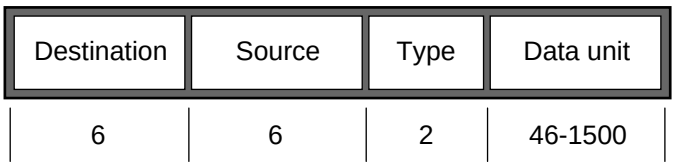
  The following figure illustrates the Ethernet 802.3 raw frame:

Figure 5-3
Ethernet 802.3 Raw Frame



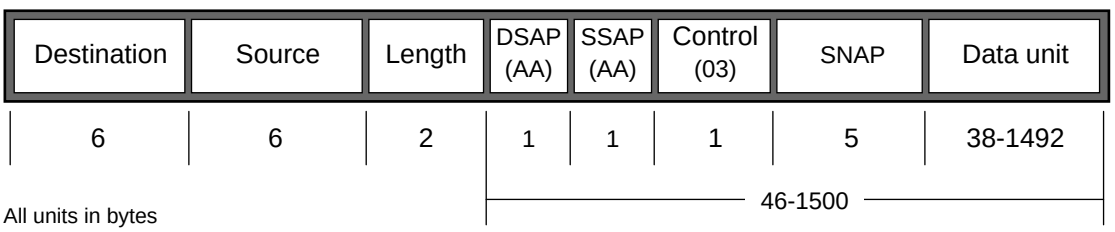
- **Ethernet II** is used on networks that communicate with DEC* minicomputers, and on computers that use TCP/IP. The following figure illustrates the Ethernet II frame:

Figure 5-4
Ethernet II Frame



- **Ethernet SNAP** is the IEEE standard 802.2 frame type with an extension (SNAP) added to the header. Used on networks that communicate with workstations using protocols such as AppleTalk Phase II. The following figure illustrates the Ethernet SNAP frame:

Figure 5-5
Ethernet SNAP Frame

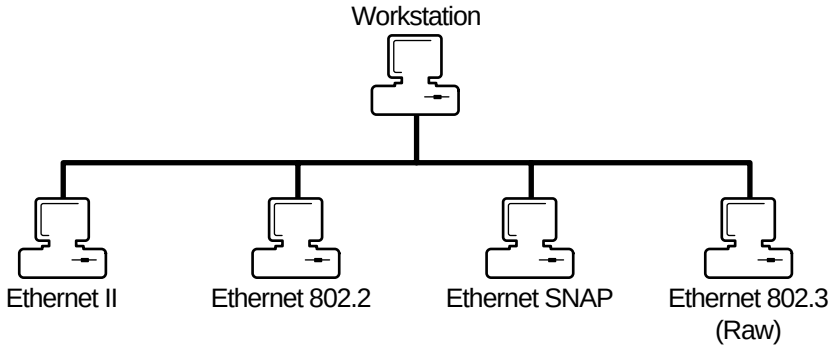


Note

On Ethernet 802.2, Ethernet II, and Ethernet SNAP cabling systems, stations using different protocol numbers *can* coexist, but they *cannot* communicate directly with each other. The 802.3 raw frames are able to communicate with other frames using an internal IPX router in the server.

Using Novell ODITM technology, NetWare 4 allows stations with different Ethernet frame types to coexist on the same Ethernet cabling system, as in the following figure:

Figure 5-6
Coexisting Frame Types



Because of the ODI Multiple Link Interface DriverTM (MLID) and Link Support LayerTM (LSL), a single workstation with one network board can communicate with other devices using different types of Ethernet frames.

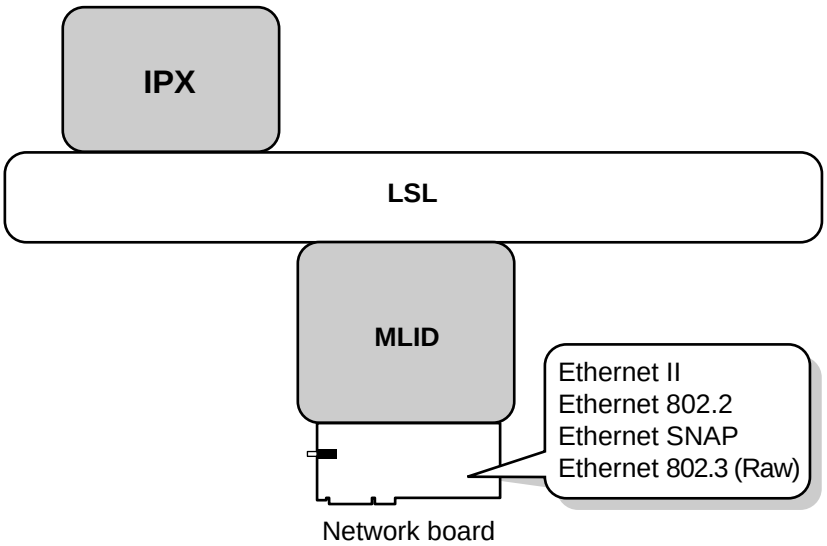
Even though there may be only one physical network board in the computer, the MLIDTM gives the effect of having multiple network boards and multiple LAN drivers.

Unlike traditional dedicated LAN drivers, the MLID is responsible for removing the media-specific (frame-specific) information from the data packets it receives.

The packets are then passed on to the LSLTM, which functions much like a switchboard operator, sending the packet to the assigned protocol stack (such as IPX).

The following figure illustrates the ODI architecture in a multiple Ethernet frame configuration using IPX protocol.

Figure 5-7
ODI Architecture Using Multiple Ethernet Frames



See also “Open Data-Link Interface” ; “Multiple Link Interface Driver” ; “Link Support Layer” ; “Packet.”

Execute Only (X) attribute

A file system attribute that prevents a file from being copied.

See also “Attributes.”

Exterior Gateway Protocol

(EGP) A protocol that exchanges network reachability information between autonomous systems. EGP is part of the TCP/IP protocol suite.

Routers within each autonomous system are chosen to use EGP to talk to the outside world, usually over the Internet. These EGP routers are called *exterior routers* .

The exterior routers become EGP neighbors. The EGP neighbors exchange information about the networks that can be reached within the neighbors' respective autonomous systems.

See also “Autonomous system.”

External Entity object

A leaf object that represents a non-native NDS object that has been imported into NDS or registered in NDS.

NetWare Message Handling ServiceTM (NetWare MHS) uses External Entity objects to represent users from non-NDS environments and provides an integrated address book for sending mail.

For example, if your messaging environment contains non-NetWare MHSTM messaging servers, such as SMTP hosts, SNADS nodes, or X.400 Message Transfer Agents, you might choose to add users and lists at these servers to your Directory database. You would add them as External Entity objects.

Adding these objects to the Directory database as External Entity objects adds them to the address books of your messaging applications. So, when addressing messages, NetWare MHS users can choose non-NetWare MHS users and lists from a directory list.

An External Entity object has an External Name property that specifies the native name that the External Entity is known by in its native messaging environment.

An External Entity also has a Foreign E-mail Address property that specifies the user's mailbox in a foreign messaging system.

See also “NetWare MHS Services.”

Chapter 6 *F*

Fake root

A subdirectory that functions as a root directory, allowing you to assign users rights at the subdirectory level.

Note

Fake roots work with NetWare shells included with NetWare 3.

Some applications can't be run from subdirectories; they read files from and write files to the root directory. However, for security, you should not assign users rights at the root or volume directory level.

NetWare allows you to map a drive to a fake root (a directory where rights can be assigned to users).

Thus, to use an application that must be installed at the root, load the files in a subdirectory and designate it as a fake root directory in the login script using MAP ROOT.

You can't 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, remap the drive.

Related utility: MAP in *Utilities Reference* .

See also "Security."

FAT

(File Allocation Table) An index table that points to the disk areas where a file is located.

See also "File Allocation Table."

Fault tolerance

A means of protecting data by reconciling bad disk blocks or by providing data duplication. (See “System Fault Tolerance.”)

Also, distributing the Directory database among several servers to provide continued authentication and access to object information should a server go down. (See “Novell Directory replica.”)

File Allocation Table

(FAT) An index table that points to the disk areas where a file is located. Because one file may be in any number of blocks spread over the disk, the FAT links the file together.

Each volume contains a FAT. The NetWare operating system divides each volume into disk allocation blocks that can be configured to 4, 8, 16, 32, or 64 KB. (All blocks on one volume are the same size.)

NetWare stores files on the volume in these blocks. If a file consists of one or more blocks, the file may be stored in blocks that aren't adjacent.

Entries in the FAT correspond to the blocks for that volume. The first entry in the FAT corresponds to the first block on that volume, the second entry corresponds to the second block, etc.

The FAT is accessed from the DET. It is cached in server memory, allowing the server to quickly access the data.

Turbo FAT index. When a file exceeds 64 blocks (and the corresponding number of FAT entries), NetWare creates a turbo FAT index to group together all FAT entries for that file.

See also “Turbo FAT index.”

File caching

The use of NetWare server RAM to improve file access time.

See “Cache memory.”

File compression

A means of allowing more data to be stored on server hard disks by compressing (packing) files that aren't being used.

By enabling NetWare volumes to be compressed, you can effectively increase disk space up to 63%. For example, 600 MB of files on a volume can be compressed to as little as 222 MB.

File compression is managed internally by the NetWare operating system. Users can flag their files or directories so they are compressed after being used, or flag them so they are never compressed.

After compression is enabled, files flagged Immediate Compress (Ic) are compressed immediately; other files are automatically compressed when they haven't been accessed for a specific amount of time. Files are decompressed when a user accesses them again.

In simplified terms, file compression works like this:

1. The file to be compressed is read and analyzed.
2. A temporary file is built describing the original file.
3. The system determines if any disk sectors are saved by compressing the file.
4. The creation of the compressed file begins.
5. After an error-free compressed version of the file is built, the original and compressed files are swapped.

If a disk error or a power failure occurs during compression, the original file is retained.

File compression is a background process that only minimally impacts server performance. However, we recommend running compression when the server is relatively idle.

You can enable file compression during or after installing NetWare 4. Once enabled, you cannot disable file compression without re-creating the volume. You can, however, temporarily suspend file compression using a SET command.

If you suspend file compression, you may have many files to be compressed once you enable file compression. If so, to avoid server performance degradation, set parameters to compress files during hours that don't affect production.

See also "Attributes."

File handle

A number used to refer to or identify a file.

File indexing

The method of indexing FAT entries for faster access to large files.

For example, if you want to go to block 128 of a file, file indexing allows you to go right to the block instead of scanning through the 127 previous blocks.

NetWare 4 supports automatic file indexing after 64 blocks.

The two levels of file indexing in NetWare 4 refer to the size of the table it uses to index the FAT.The first level indexes 64 to 1,023 blocks; the second level, 1,024 or more blocks.

See also "File Allocation Table."

File rights

Rights that control what a trustee can do with a file.

See "Rights."

File Scan right

A file system right that grants the right to see the directory and file with the DIR or NDIR directory command.

See also "Rights."

File server

A name used in previous NetWare versions for the computer that runs NetWare operating system software; now referred to as the *NetWare server* .

See “NetWare server.”

File system

(Formerly *directory structure*) The system the NetWare server uses to organize data on its hard disks. Each file is given a filename and stored at a specific location in a hierarchical filing system so that files can be located quickly.

Note

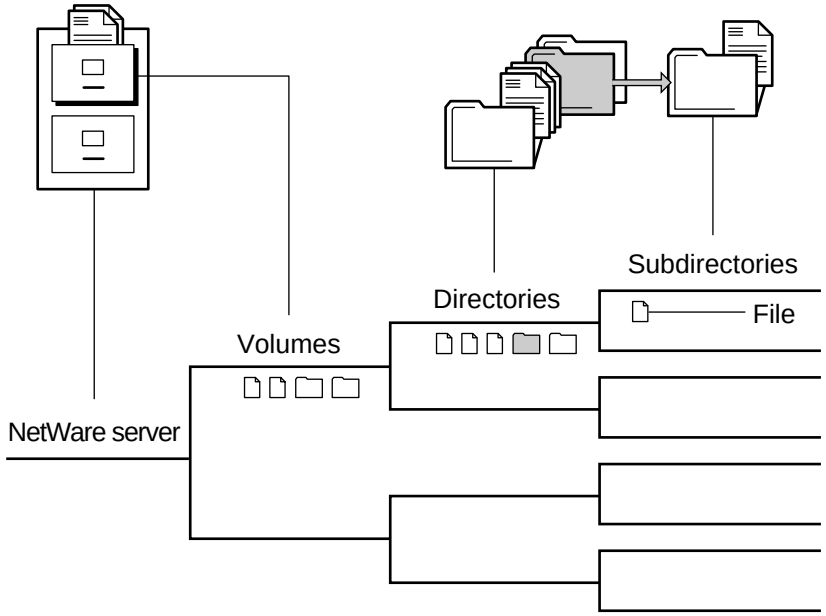
In previous NetWare versions, this concept was referred to as *directory structure.* The concept is now called *file system* to distinguish it from the Directory that is part of NDS.

The NetWare server is divided into one or more volumes. Volumes are divided into directories containing files or subdirectories.

The file system is analogous to an office filing system, as illustrated in the following figure.

Figure 6-1

Volumes, Directories, and Files



Volume is the highest level in the NetWare file system, created from logical partitions using INSTALL. A volume can reside on one hard disk, or it can span multiple hard disks.

To a user, a volume appears much like a hard disk in a standalone system.

You can store directories at the volume level. Storing files at this level is possible but, for security reasons, isn't recommended.

Directory is a place within a volume where you can store files or other directories. Directories within directories are called *subdirectories* .

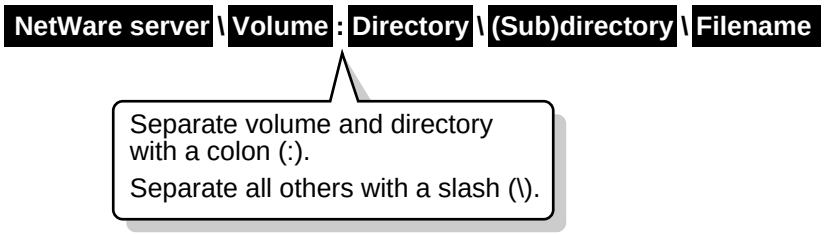
A directory can contain any number of files and subdirectories.

Files are individual records that can be created in or copied to any level of the directory structure (except, in practice, the volume level).

Directory Path

A file or directory is located by its *path* , which states where the directory or file is on a volume. The following figure shows how to specify a path. (Listing the server is optional.)

Figure 6-2
Directory Path Conventions



Under DOS, directory names and filenames contain one to eight characters, followed with an optional filename extension.

If your network uses more than one client operating system, keep in mind the conventions of the different systems. For example, NetWare allows 255 characters in a directory path (counting the drive letter and delimiters), but DOS permits only 127 characters.

Also, some applications restrict the number of characters in the directory path. For more information, check the application's documentation.

Basic NetWare Server Directories

When volume SYS: is created, it contains seven predefined directories:

- **SYS:DELETED.SAV** Holds files that have been deleted until they are purged.
- **SYS:ETC** Contains sample files to assist the network supervisor in configuring the server.
- **SYS:LOGIN** Contains programs necessary for users to log in.
- **SYS:MAIL** Is used by mail programs compatible with NetWare. (NetWare creates a subdirectory in SYS:MAIL for User object ADMIN.)

If you upgrade from an earlier NetWare version, existing users still have subdirectories here, but their login script becomes a property of their User objects.

If you create new users after upgrading, the new users do not have directories in SYS:MAIL.

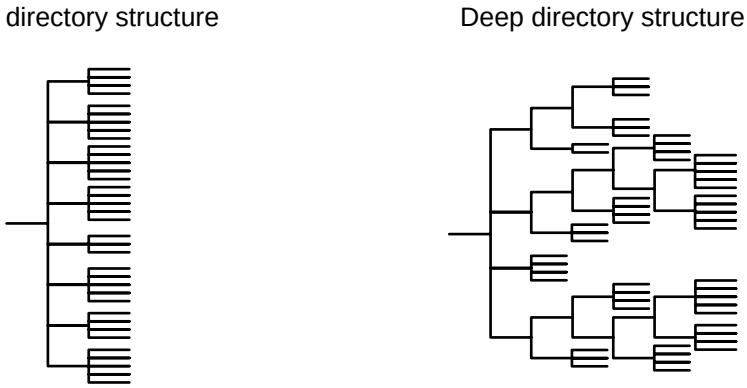
- **SYS:SYSTEM** Contains NetWare operating system files as well as NLM programs and NetWare utilities used for managing the network.
- **SYS:PUBLIC** Allows general access to the network and contains NetWare utilities and programs for network users.
- **SYS:DOC** Contains electronic versions of the NetWare manuals.

Directory Structures

All directories are organized in tree structures, but a directory structure can be flat with many directories coming off the volume, or it can be deep with several levels of directories.

The following figure illustrates possible directory structures:

Figure 6-3
Flat and Deep Directory Structures



The general principle is to keep directory structure clean and logical. Keeping the structure relatively flat (no more than five levels deep) generally increases usability.

Directory Types

You can create directories for both executable files and data files, depending on what types of directories best fit the needs of your network.

Operating system directories Store workstation operating system files.

The number of DOS or other operating system directories you need depends on the number of different operating systems, versions, and workstation types on the network.

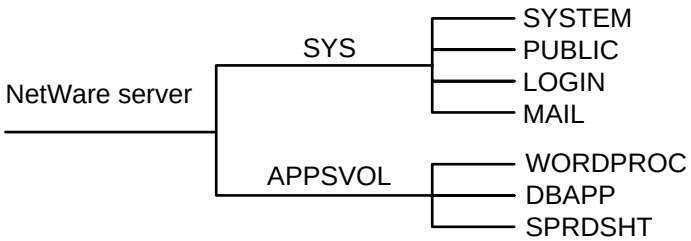
Application directories Contain applications that can be accessed from local drives; installing them on the network provides convenient access.

Several structures are possible for application directories:

- Create a separate volume for applications, with a separate directory for each application off the root. Make trustee assignments for each application. Then go into the system or profile login script and map a search drive to each application.

  The following figure shows this type of directory structure:

Figure 6-4
Application Volume

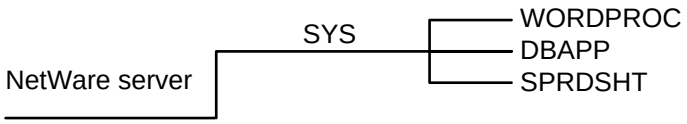


- Create a separate directory off volume SYS: for each application. Make trustee assignments for each application. Then go into the system or profile login script and map a search drive to each application.

  The following figure shows this type of directory structure.

Figure 6-5

Application Directory off Volume SYS:

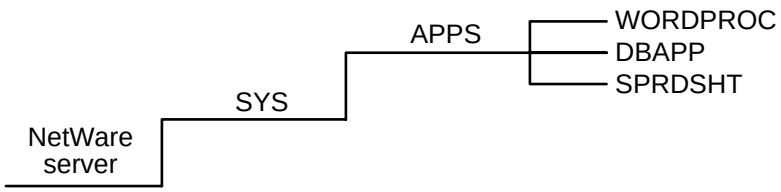


- Create a parent directory for applications, with subdirectories for each application. Make trustee assignments for each application. Then go into the system or profile login script and map a search drive to each application.

  The following figure shows this type of directory structure.

Figure 6-6

Parent Directory for Applications



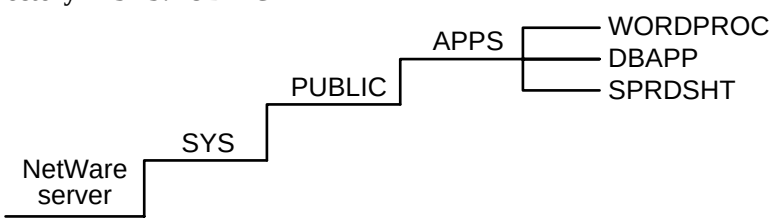
- Create a parent directory for applications in SYS:PUBLIC.

  Because users generally have Read and File Scan rights in SYS:PUBLIC, you don't need to make trustee assignments or map a search drive. However, users can see and use all applications.

  Use this directory structure only if you want all users to have access to all applications. The following figure shows this type of directory structure.

Figure 6-7

Application Directory in SYS:PUBLIC



Installing applications in SYS:PUBLIC isn't recommended (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. If so, one file overwrites the other because two files with the same filename can't coexist in a directory.

Note

Some applications write files to the root. For security reasons you don't want users working at the root level. Therefore, use MAP ROOT to map a drive to a fake root—a directory or subdirectory in which the user can be assigned rights (See "Fake root.")

Data directories Are work directories for groups and users to keep work files in. You can also create a directory to transfer files between directories on the network.

Although data can be created and stored in a home or user directory, when data is stored in a user's directory, no other user (except network supervisors or managers assigned file rights) can access it.

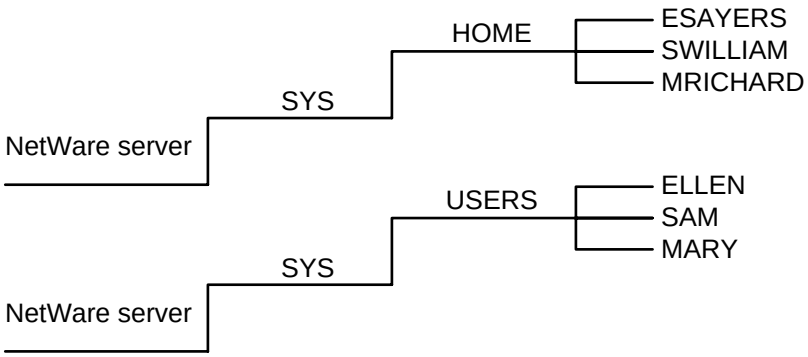
So, to allow users to share data, create work directories and make trustee assignments for groups or users who need access to these directories.

Home or username directories Are used to provide personal workspace for users.

You can create a parent directory in volume SYS: called HOME or USERS. Or, you can create a separate HOME or USERS volume. 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 displays only 8 characters in a one-level directory name. The following figure shows this type of directory structure.

Figure 6-8
Home or Username Directories



Related utilities: FILER , MAP , NLIST , NETADMIN , and RENDIR in *Utilities Reference* .

Related DOS utilities: CD (Change Directory); DIR; MD (Make Directory); RD (Remove Directory). See your DOS manual.

See also “Directory” ; “Directory Entry Table” ; “Drive mapping” ; “Security.”

File Transfer Protocol

(FTP) A set of control procedures to prevent errors in information transmitted between network stations. FTP is part of the TCP/IP protocol suite.

The data is sent from one station to another in packets. Each packet includes a discrete number that is derived from the data that makes up the packet, according to a mathematical algorithm.

The algorithm is applied to each data packet a second time when it arrives on the receiving end.

If the number on the receiving end doesn't match the number included in the packet, the receiving station sends a signal to the transmitting station requesting that the packet be resent.

Foreign e-mail address

Specifies an object's mailbox that resides in a foreign e-mail system.

For example, an NDS user can choose to have e-mail delivered to a UNIX machine that supports the SMTP messaging protocol. This user's SMTP address in the UNIX machine (the SMTP native name) is also the user's foreign e-mail address.

An object can have only one foreign e-mail address.

Foreign e-mail alias

Specifies an object's aliases as known in a foreign messaging system.

A foreign e-mail alias is the return address value used when the NetWare MHS user sends e-mail to an X.400 user.

For example, a NetWare MHS user (a user whose mailbox is located on an MHS Messaging Server) can have an X.400 alias—with an X.400 native name—so that X.400 users can use this alias to send mail to the MHS user.

An object can have several foreign e-mail aliases, one for each type of foreign e-mail system.

Frame

A packet data format for a given media.

Some media support multiple packet formats (frames), such as Ethernet 802.2, Ethernet 802.3, Ethernet II, Ethernet SNAP, token ring, or token ring SNAP.

For NetWare 4, the default Ethernet frame type is 802.2.

See also "Ethernet configuration."

FTP

(File Transfer Protocol) A set of control procedures to prevent errors in information transmitted between workstations. FTP is part of the TCP/IP protocol suite.

See "File Transfer Protocol."

Chapter 7 *G*

Gateway

A link between two networks.

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

Group object

A leaf object that represents a grouping of several User objects, used to provide collective, rather than individual, network administration.

For example, whenever electronic mail is sent to a Group object, or whenever a trustee assignment names a Group object, each user in the list is part of that action.

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

You can use Group objects to simplify trustee assignments. For example, instead of repeating a trustee assignment for each user, you can create a Group object that lists the users and then grant the trustee assignment to the Group.

Related utilities: FILER , NETADMIN , and NetWare Administrator in *Utilities Reference* .

See also “Effective rights” ; “Object” ; Managing Group Objects in *Supervising the Network* .

Chapter 8 *H*

HAM

(Host Adapter Module) A driver component used to drive specific host adapter hardware in NWPA.

The HAM adapter drivers have a .HAM file extension.

See “NetWare Peripheral Architecture.”

Handle

A pointer used by a computer to identify a resource or feature.

For example, a directory handle identifies a volume and a directory, such as SYS:PUBLIC.

Other types of handles used to access NetWare 4 include file handles, video handles, request handles, device handles, and volume handles.

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 and read data. Hard disks can be network or local workstation disks.

Internal disks use channel 0 and external hard disks use channels 1 through 4.

See also “Data protection” ; “Disk driver” ; “Host Bus Adapter” ; “Partition (disk).”

Hashing

A process that facilitates access to a file in a large volume by calculating the file's address both in cache memory and on the hard disk.

See also “Cache memory.”

HBA

(Host Bus Adapter) A board that acts as an interface between the host microprocessor and the disk controller.

See “NetWare Peripheral Architecture.”

HCSS

(High Capacity Storage System) A system that increases data storage capacity by integrating an optical disc library into the NetWare file system.

See “High Capacity Storage System.”

Hexadecimal

A base-16 numeric notation system 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 characters A through F (A = decimal 10, B = decimal 11, etc.).

Hidden (H) attribute

A DOS attribute that hides a directory or file from the DOS DIR command and prevents the directory or file from being deleted or copied.

See also “Attributes.”

High Capacity Storage System

(HCSS) A data storage system that extends the storage capacity of a NetWare server by integrating an optical disc library, or *jukebox* , into the NetWare file system.

HCSS moves files between faster low-capacity storage devices (the server's hard disk) and slower high-capacity storage devices (optical discs in a jukebox).

This process is transparent to the user; the file still appears to be stored on the file server.

Users and programs can access files and directories on a jukebox using the same NetWare commands and function calls used to access them from the hard disk.

HCSS uses rewritable optical discs. By using rewritable disks, data can be repeatedly written and erased. An optical disc can be one-sided or two-sided.

Data Migration and Demigration

HCSS uses free space on the server's hard disk to temporarily cache the jukebox's most active files.

When space on the hard disk reaches a preconfigured capacity, the cache's least active files are moved to optical discs. This process is known as data *migration* .

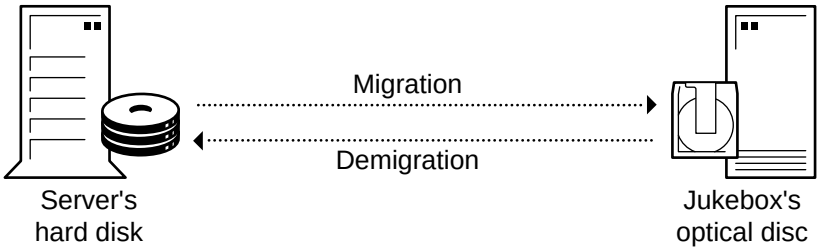
When a user requests a file and that file was migrated to an optical disc, HCSS copies the file from the jukebox onto the server's hard disk.

This process, known as *demigration* , allows users to access their least active files in the same manner as their most active files, with only a slight delay in response time.

The path name of a file remains the same whether the file resides on the hard disk or on optical disc.

The following figure demonstrates the processes of migration and demigration.

Figure 8-1
Migration and Demigration of the Requested File



Data migration and demigration allow HCSS to optimize the use of the server's storage devices. Migration is performed on a file-by-file basis, according to the amount of hard disk space used (capacity threshold) and the last time a file was accessed (least recently used).

- **Capacity threshold** is the percentage of the server's hard disk that can be used before HCSS starts migrating files from the hard disk to the jukebox.

- **Least recently used** is the rule that determines which files are moved from the server's hard disk to the jukebox. The least active files are the first moved.

HCSS Directory Management

An HCSS directory is a file system directory that logically groups one or more optical discs and its associated files. An HCSS directory resides on the NetWare volume that is associated with the directory's jukebox.

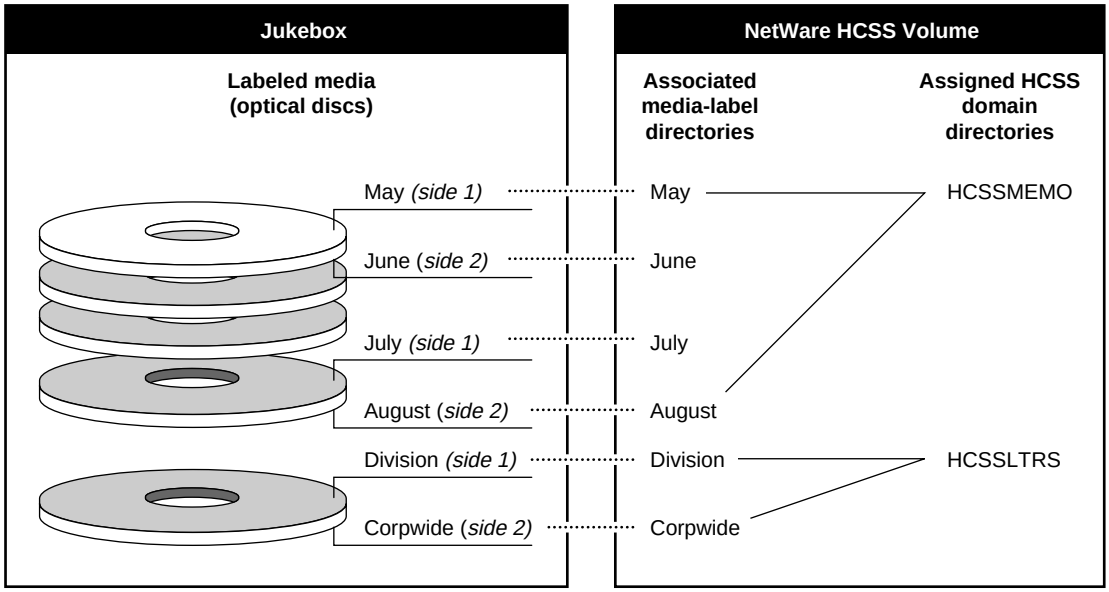
The network supervisor can create one or more HCSS directories for each jukebox.

The network supervisor assigns unique labels to each side of each optical disc, and then assigns each optical disc to an HCSS domain directory. Once

assigned, each label appears as a media-label directory within the HCSS directory.

The following figure shows the association between labeled media (magneto-optical media) and the media-label directories.

Figure 8-2
Media Grouped into HCSS Directories



An HCSS directory's contents can be viewed using any directory listing command (such as the DOS DIR or NetWare NDIR commands).

Users can access and manipulate HCSS first-level subdirectories the same way they access any other NetWare directory, except that users can't create or delete an HCSS first-level subdirectory.

Access control rights are assigned to HCSS directories in the same way they are for other NetWare directories.

See also "Data migration."

Home directory

A private network directory that the network supervisor can create for a user. Users' login scripts should contain a drive mapping to their home directories.

Hop count

The number of cable segments a message packet passes through on the way to its destination on a network or internetwork.

The destination network can be no more than 16 hops from the source.

The server utilities DISPLAY NETWORKS, DISPLAY SERVERS, and TRACK ON show how many hops other recognized networks are from the server router.

They also show the number of ticks (1/18 of a second) it takes for the message packet to reach its destination network.

See also “Partition (disk).”

Host

A NetWare server from which you run SBACKUP. A storage device and a storage device controller are attached to it.

See also “Backup” ; “Target.”

Host Adapter Module

(HAM) The driver component used to drive specific host adapter hardware in NWPA.

See “NetWare Peripheral Architecture.”

Host Bus Adapter

(HBA) A SCSI adapter board or disk controller that adds a bus through which peripheral devices (such as hard disks, tape drives, and CD-ROM drives) are connected to the computer.

These devices typically have embedded controllers.

See also “Hard disk” ; “SCSI bus.”

Hot Fix

A method NetWare uses to ensure that data is stored safely. Data blocks are redirected from faulty blocks on the server's disk to a small portion of disk space set aside as the *Hot FixTM Redirection Area* .

Once the operating system records the address of the defective block in a section of the Hot Fix area reserved for that purpose, the server doesn't attempt to store data in defective blocks.

By default, 2% of a disk partition's space is set aside as the Hot Fix Redirection Area.

Hot Fix is always active unless the disk fails and is inoperative, or unless the redirection area is full. Hot Fix, together with read-after-write verification, enables a hard disk to maintain data integrity.

See also "Data protection."

Hub

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

Two kinds of hubs exist:

- **Active hubs** amplify transmission signals in network topologies. Use active hubs to add workstations to a network or to extend the cable distance between stations and the server.

- **Passive hubs** are used in certain network topologies to split a transmission signal, allowing additional workstations to be added. Passive hubs can't amplify the signal, so it must be cabled directly to a station or to an active hub.

Chapter

9 *I*

ICMP

(Internet Control Message Protocol) A protocol in the TCP/IP suite that sends packets containing information about network failures, such as inoperative nodes and gateways, or congestion at a gateway.

See “Internet Control Message Protocol.”

IDE

A hard disk drive standard interface.

See also “Integrated Drive Electronics.”

Identifier variables

Variables used in login scripts that allow you to enter a variable (such as LOGIN_NAME) in a login script command, rather than specific information (such as RICHARD).

See “Login scripts.”

I’m Alive packet

Diagnostic packets SFT III servers send back and forth over the internetwork connection to check each other's status.

Each SFT III server sends an I'm alive packet to the other SFT III server over the IPX cable at a rate of 18 times per second. These packets act as a backup communications check for the mirrored server link.

A network analyzer attached to the LAN segment between the two SFT III servers detects many I'm alive packets per minute. However, the extra traffic generated by these diagnostic packets should not affect network performance.

Immediate Compress (Ic) attribute

A file system attribute that causes files to be compressed as soon as the operating system can do so. The operating system doesn't wait for a specific event (such as a time delay) before compressing the file.

See also "Attributes."

Indexed (I) attribute

A status flag set automatically when a file exceeds a set size, indicating that the file is indexed for fast access.

See also "Attributes."

Inherited Rights Filter

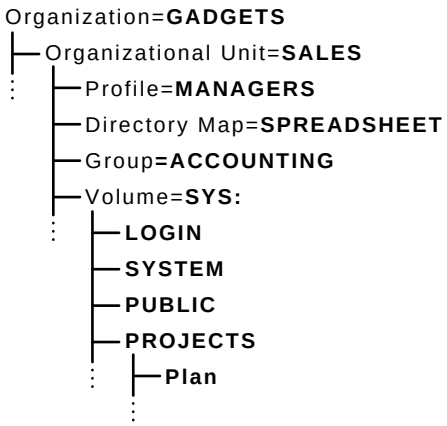
(IRF) A list of rights created for every file, directory, and object. The IRF controls the rights that a trustee can inherit from parent directories and container objects.

By default, the IRF allows every right to be inherited from the parent directory or container object. The IRF cannot grant rights, it can only allow or revoke rights.

To allow a right, the right must exist in the parent directory or container object and the IRF.

To revoke a right, the right must exist in the parent directory or container object and then be removed from the IRF.

The IRF is ignored whenever a trustee has an explicit trustee assignment to that file, directory, or object.



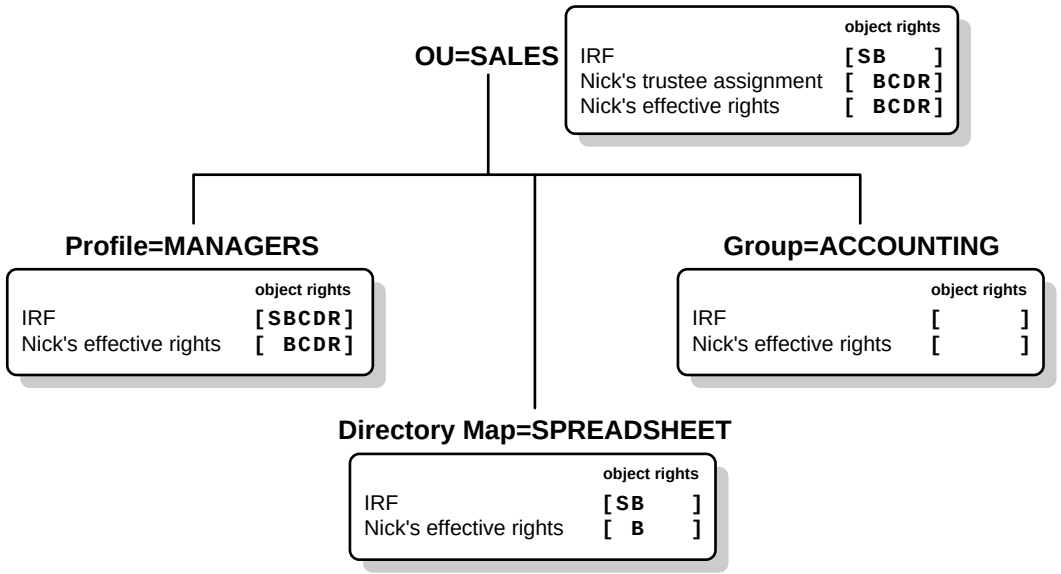
Use this figure as a reference for “Inherited Rights Filter” and “Effective Rights Chart.” . Together, they show how a trustee assignment flows through the IRF to determine which rights the trustee can exercise within a file, directory, or object.

Figure 9-1 illustrates the effective rights of user Nick, who is assigned object and property rights to the SALES object. Nick is also granted trustee rights to the PROJECTS directory.

Nick's trustee assignment to Organizational Unit SALES grants him BCDR (Browse, Create, Delete, Rename) object rights.

Because Nick doesn't have a trustee assignment to any of the three objects within the SALES container, Nick's effective rights to those objects are inherited from SALES and must pass through the IRF of each object.

Figure 9-1
Inherited Rights Filter



Because Nick has an explicit trustee assignment to SALES, the IRF for SALES has no affect on his rights.

The IRF for MANAGERS allows all rights to pass through, so Nick's rights to MANAGERS are the same as his rights to SALES.

However, the IRFs for SPREADSHEET and ACCOUNTING block rights from SALES, so Nick doesn't have the same rights for those objects.

If Nick is granted an explicit trustee assignment to any objects below SALES, the IRF for those objects is ignored and his new assignment determines his effective rights.

Figure 9-2 lists the results of these rights flowing through the IRFs.

Figure 9-2
Effective Rights Chart

Directory and File System Objects	Trustee Assignments	IRF	Effective Rights
OU=SALES	Object=[BCDR] All Properties=[CRW]	[SB] [RW]	[BCDR] [CRW]
Profile=MANAGERS		[SBCWR] [SCRWA]	[BCDR] [CRW]
Directory Map= Spreadsheet		[SB] [SCRWA]	[B] [CRW]
Group= ACCOUNTING		[ ] [ ]	[ ] [ ]
Directory= PROJECTS	[RWCE F]	[SR]	[RWCE F]
File=Plan		[SR C F]	[R C F]

Note

Only rights assigned for all properties can be inherited. Rights assigned to selected properties can't be inherited. (See “Rights.”)

Blocking the Supervisor Object Right

The IRF of an object and its properties can block the Supervisor object right. This allows distributed management of the Directory tree.

However, NetWare utilities don’t allow you to block the Supervisor object right unless an object, including itself, is already granted the Supervisor right to that object. This helps to prevent cutting off Supervisor-level access to a part of the Directory tree.

Warning

Any object can be assigned as a trustee to an object, including to itself. But unless the trustee assignment is a User object, blocking the Supervisor object right with the IRF still cuts off that object from future control because you can only log in as a User object.

Because the Supervisor right to objects and properties can be blocked, you should also grant a trustee all other rights.

For example, don’t grant only the Supervisor right. Even though that right allows or implies all rights to an object, if the Supervisor right is blocked, the trustee is left with no rights.

Instead, grant all rights to the trustees, so that if Supervisor is blocked by an IRF, the trustee still has Browse, Rename, Create, and Delete rights.

To change the IRF of an object, you must have at least the Write property right to the ACL property of that object.

As with previous versions of NetWare, the Supervisor right cannot be blocked in the file system. A trustee who has the Supervisor right in the root directory of a volume has the Supervisor right to the entire volume, and it cannot be blocked with an IRF.

Changing the IRF

The IRF for any file, directory, or object is part of the access control list (ACL) for that file, directory, or object.

To change the IRF of an object, you must have at least the Write property right to the ACL property of that object.

To change the IRF of a file or directory, you must have the Access Control right to that file or directory.

Related utilities: FILER , NETADMIN , NetWare Administrator , and RIGHTS in *Utilities Reference* .

See also “Effective rights” ; “Security.”

Input/Output Engine

The part of the SFT III operating system that handles physical processes, such as network and disk I/O, hardware interrupts, device drivers, timing, and routing

See “IOEngine.”

Integrated Drive Electronics

(IDE) A hard disk drive standard interface. The IDE integrates controller electronics onto the drive.

The controller connects to a paddleboard that may be external to, or on, the motherboard. The paddleboard then interfaces with the bus to the CPU.

Unlike the IDE drive, the SCSI drive has a separate host bus adapter (HBA) instead of the paddleboard. The HBA interfaces with the bus to the CPU.

You can identify an IDE bus by its 40-pin connector, as opposed to a SCSI bus, which has a 50-pin connector.

See also “Hard disk.”

Internal network number

A logical network number that identifies an individual NetWare 3 or NetWare 4 server.

On IPX networks the internal network number must also be different from the IPX external network number.

See also “IPX internal network number” ; “IPX external network number.”

International use of NetWare 4

The adaptation of NetWare 4 for use with multiple languages.

The NetWare 4 operating system, NLM programs, and utilities use English as the default language but can be set to several other languages.

You can have NLM programs running in different languages at the same time.

The formats for expressing dates, times, and numbers also change across languages, and sometimes change across locales within a given language area.

In NetWare 4, you can configure certain local formats through INSTALL.NLM. You specify the formats when installing the NetWare server, but you can reconfigure these formats with INSTALL.NLM while the server is running.

You can configure the following information:

- Date

- Time
- Currency
- Sorting tables
- Upper case tables
- Supported filename characters

The following are some formats for various locales:

Table 9-1

Location	Date	Time	Number
USA	06/19/94	8:37:00 PM	12,345.67
UK	19/06/94	20:37:00	12,345.67
France	19.06.94	20:37:00	12 345,67
Germany	19.06.94	20:37:00	12.345,67

Languages Supported

NetWare 4 supports the following languages:

- German
- French
- Italian
- Spanish

You can set the language for the following:

- Server
- Message files
- Console keyboard

Setting the Language of the Server

You must set the server language when loading SERVER.EXE. Setting the language later requires you to reboot the NetWare server.

The server language is determined by the SERVER.MSG file.

See Setting a Server's Language in *Supervising the Network* .

Setting the Language of the Message Files

You must specify the language you want NLM messages to be displayed in. To set the language for the message file, use the LANGUAGE.NLM.

You can change the language for NLM messages anytime. It is not necessary to reboot the server.

See Specifying a Language for an NLM in *Supervising the Network* .

Setting the Language of the Console Keyboard

Set the server keyboard type by loading KEYB.NLM and executing the **KEYB** console command.

You can change the keyboard type anytime. It is not necessary to reboot the server.

See Changing the Server Keyboard Type in *Supervising the Network* .

Internet Control Message Protocol

(ICMP) A protocol in the TCP/IP suite that sends packets containing information about failures on the network such as inoperative nodes and gateways, and congestion at a gateway.

IP software interprets and acts on an ICMP message. Because an ICMP message might need to travel across several networks to reach its destination, it is encapsulated in the data portion of an IP datagram.

See also "Internet Protocol" ; "TCP/IP."

Internet Protocol

(IP) The network layer protocol of the TCP/IP suite of protocols. IP enables dissimilar nodes in a heterogenous environment to communicate with one another.

See also “TCP/IP.”

Internetwork

Two or more networks connected by a router. Each network has a unique network number.

Users on an internetwork can use the resources (files, printers, hard disks) of all connected networks, provided they have security clearance.

See also “Router” ; “IPX external network number.”

Interoperability

The ability to use products from different vendors within the same system.

For example, Novell ODINSUP interface allows LAN Manager, LAN Server, or other NDS protocols to co-exist with ODI on a network.

Communication protocols, such as IP or AFP, can be used in ODI to process information from the network without the user having to know each protocol's required method of packet transmission.

Interoperability also means that an application running on different platforms (such as UNIX) can share files.

See also “Open Data-Link Interface” ; “ODINSUP.”

Interrupt mode

A printer configuration option through which the data port sends a signal, or interrupt, to the port driver (NPRINTER) when it is ready to accept another character to be transmitted to the printer. The interrupt instructs the CPU to

suspend its other processing activities to service the needs of the port in question.

In past releases of NetWare, using interrupt mode was faster than the alternative polled mode.

However, the enhanced performance of NPRINTER for NetWare 4 makes polled mode considerably faster than before. In most instances, users see little difference in performance.

Also, using interrupt mode has the disadvantage of possible interrupt conflicts among different devices attempting to access the same processor.

See also “Polled mode.”

IOEngine

(Input/Output Engine) The part of the SFT III operating system that handles physical processes, such as network and disk I/O, hardware interrupts, device drivers, timing, and routing.

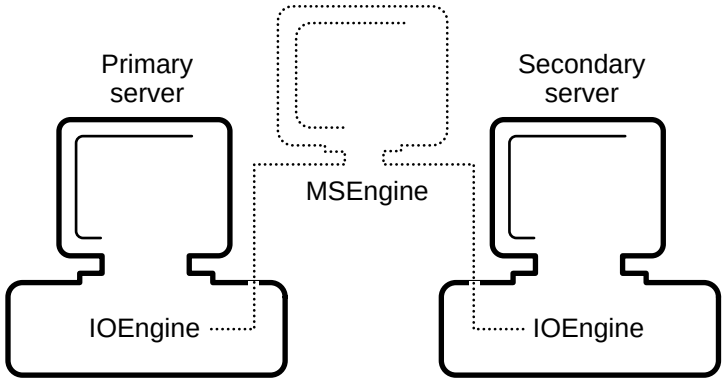
SFT III is split into two parts: the IOEngine and the MSEngine (Mirrored Server Engine). The IOEngine routes packets between the network and the MSEngine.

To network workstations, the IOEngine appears as a standard NetWare router or bridge (making the SFT III server at least two hops away from any other router or workstation). The primary server and the secondary server each have an IOEngine, but they share the same MSEngine.

Because the IOEngines are not mirrored, NLM programs and applications that directly interface with hardware, such as NPRINTER.NLM, are not mirrored.

Hardware-related applications and NLM programs must be installed in the IOEngines on both the primary and secondary server.

Figure 9-3
IOEngine and MSEngine



IP address

Identifies the network to which the host server is attached.

The address is normally in four segments, each separated by a period (for example, 87.34.53.12). Individual numbers must be between 0 and 255.

IP tunneling

A method by which two or more IPX networks exchange packets through an IP internetwork.

The tunnel sends each IPX packet across the IP internetwork by encapsulating it in a User Datagram Protocol (UDP) datagram.

The tunnel driver at the destination removes the UDP header from each incoming packet and passes it through the ODI to IPX.

IPX

(Internetwork Packet Exchange) A Novell communication protocol that sends data packets to requested destinations (such as workstations or servers).

IPX allows packet addressing within a single network, or in an internetwork environment. (That is, two or more networks connected by a router, where each network has a unique IPX external network number.)

Through IPX, incoming data packets are directed to the proper area within the operating system of the workstation or NetWare server.

IPX provides services to help other network-aware programs in their network data-transmission process.

The IPXODI.COM file then uses the services of a LAN driver routine to control the station's network board for data delivery.

Thus, IPX allows data packets to be sent and received through physically different networks and workstations.

See also "Communication protocols" ; "Internetwork" ; "IPXODI" ; "LAN driver"; "Open Data-Link Interface."

IPX external network number

A network number that uniquely identifies a network cable segment.

An IPX external network number is a hexadecimal number, one to eight digits (1 to FFFFFFFE). The number is arbitrary, and is assigned when the IPX protocol is bound to a network board in the server.

You can bind IPX with multiple frame types to the same network board.

For example, the installation utility can install both Ethernet Raw 802.3 and IEEE 802.2 frame types as defaults and bind the IPX protocol stack to each.

Both frame types are represented as logical IPX networks, and the IPX router, which is internal to the operating system, routes packets between the two logical networks.

This means that each frame type requires its own unique logical IPX external network number, even though both frame types are bound to the same network board and physical cable segment.

The terms *network number* and *network address* are sometimes used to refer to the IPX external network number.

See also "IPX internal network number" ; "IPX internetwork address" ; "Network numbering."

IPX internal network number

A logical network number that identifies an individual NetWare server. The IPX internal network number is a hexadecimal number, one to eight digits (1 to FFFFFFFE), and is assigned to the server during installation.

Each server on a network must have a unique IPX internal network number. The IPX internal network number of any node must also be different from any IPX external network number on the internetwork.

In earlier versions of NetWare, the IPX internal network number was referred to as the *internal network number.*

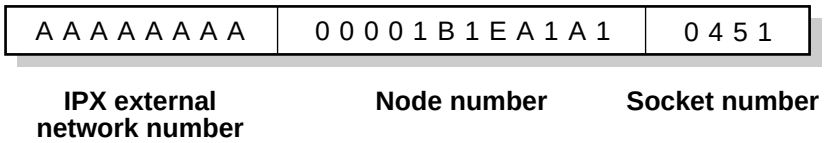
An internal network (used in NetWare 3 and NetWare 4) is a *logical* network that routes packets to the physical networks that a NetWare server is attached to.

See also “AUTOEXEC.NCF” ; “IPX external network number.”

IPX internetwork address

A 12-byte number (represented by 24 hexadecimal characters) divided into three parts, illustrated in the following figure:

Figure 9-4
IPX Internetwork Address



The first part is the 4-byte (8-character) IPX external network number. The second part is the 6-byte (12-character) node number. The third part is the 2-byte (4-character) socket number.

Typically, the example address is written:

AAAAAAAA: 00001B1EA1A1; 0451.

(The leading zeros in the node number can be eliminated.)

See also “IPX external network number” ; “Node number” ; “Socket.”

IPXODI

(Internetwork Packet Exchange Open Data-Link Interface) A module that takes the workstation requests the DOS Requester has determined are for the network, packages them with transmission information (such as their destination), and transfers them to the LSL.

IPXODI requires that each packet has an initialized header. The header specifies information that targets network delivery, announcing where the packet came from, where it's going, and what happens after delivery.

Because IPXODI transmits data packets as datagrams (self-contained packages that move independently from source to destination), it can only deliver the packets on a best-effort basis. To guarantee delivery of packets, use SPX.

See also "IPX" ; "Link Support Layer" ; "SPX."

Chapter 10 *J*

Jukebox

A high-capacity storage device, sometimes called an *optical disc library* , that uses an autochanger mechanism to mount and dismount optical discs as they are needed.

A jukebox typically contains one to four optical disc drives. A picker rotates, flips, and transports disks to and from the storage slots, drives, and the mail slot. The mail slot is the location in the jukebox used to insert and remove the optical disc cartridge.

See also “High Capacity Storage System.”

Chapter 11 *L*

LAN

(LAN) A network located within a small area or common environment, such as in a building or a building complex.

See also “Wide area network.”

LAN driver

An NLM that interfaces with a network board.

A LAN driver serves as a link between a station's operating system and the physical network parts.

NetWare 4 is designed for LAN drivers written to the Open Data-Link Interface (ODI) specification. Under this specification, the LAN driver is more specifically referred to as a Multiple Link Interface Driver (MLID).

ODI drivers connect directly to the ODI model's LSL, which serves as an intermediary between the drivers and the communication protocols.

NetWare LAN drivers have a .LAN filename extension.

See also “Link Support Layer” ; “Multiple Link Interface Driver” ; “NetWare Loadable Module” ; “Open Data-Link Interface.”

Large Internet Packet

(LIP) A functionality that allows the maximum size of internetwork packets to be increased. (Formerly, the maximum size was 576 bytes.)

In NetWare versions earlier than NetWare 4, the workstation initiated a negotiation with the NetWare server to determine an acceptable packet size.

If, during this negotiation, the server detected a router between it and the station, the server limited the maximum packet size to 576 bytes.

However, some network architecture, such as Ethernet and token ring, support packets larger than 576 bytes.

Thus, in NetWare 4, LIP allows the workstation to determine the packet size based on the maximum size supported by the router.

LIP functionality is implemented for DOS clients through the station's NET.CFG file.

See also configuring for large Internet packets in the Novell Client documentation.

Leaf objects

Objects that don't contain any other objects, located at the end of a branch in the Directory tree.

See also "Object" ; NDS Object Classes and Properties in *Guide to NetWare 4 Networks* .

License Service Provider

(LSP) An NLMTM program that responds to requests from NetWare Licensing Services (NLS) clients and licensing service managers for licensing information or license units.

You do not need to have an LSP loaded on every server. An installation of NLS requires only one LSP with access to the Directory database. However, using multiple LSPs enables NLS to be much more scalable.

See also "LSP Server object" ; "NetWare Licensing Services."

Licensed Certificate object

A leaf object used with NetWare Licensing Services (NLS) technology to install product license certificates as objects in the NetWare Directory database.

License Certificate objects are added to the Licensed Product container when an NLS-aware application is installed.

See also “Licensed Product object.”

Licensed Product object

A container object that is created automatically when you install applications enabled for NetWare Licensing Services (NLS) technology. When an NLS-enabled application is installed, it adds a Licensed Product container object to the NetWare Directory database and a License Certificate leaf object to that container.

See also “Licensed Certificate object.”

Link state

A routing algorithm that builds and maintains a logical map of the entire network.

A link state router accomplishes this by sending a packet containing information about all its links—connections to networks and other routers—to all other link state routers on the network. This process is known as *flooding* . Each router uses this information to build the network map.

When each link state router has the same view (map) of the network, the network is said to have *converged* . Link state routers multicast their link information only when a change occurs in a route or service.

See also “NetWare Link Services Protocol” ; “Open Shortest Path First.”

Link Support Layer

(LSL) An implementation of the ODI specification that serves as an intermediary between the NetWare server's LAN drivers and the communication protocols, such as IPX, AFP, or TCP/IP.

The LSL allows one network board to service several communications protocol stacks. It also allows several network boards to service the same protocol stack.

See also "Open Data-Link Interface."

LIP

(Large Internet Packet) A functionality that allows the maximum size of internetwork packets to be increased.

See "Large Internet Packet."

Loadable module

A program you can load and unload from a server or a workstation while the attendant operating system is running. The most common type is the NLM program.

See "NetWare Loadable Module".

Loading and unloading

The process of linking and unlinking NLM programs to the NetWare operating system.

NLM programs can be loaded and unloaded while NetWare is running. For precautions to take before unloading a disk or LAN driver, see UNLOAD in *Utilities Reference* .

Related utilities: LOAD and UNLOAD in *Utilities Reference* .

See also "NetWare Loadable Module."

Local area network

(LAN) A network located within a small area or common environment, such as in a building or a building complex.

See also “Wide area network.”

Local drive

A common name for a *physical drive* attached to a workstation.

See “Drive.”

Logical memory

Memory that may not have contiguous addresses, but which appears contiguous to NetWare 4 processes.

See also “Paging.”

Login

The procedure that provides access to the network by using the LOGIN command.

When a user initiates a login request, the operating system looks for security rights; the user is then asked for a password.

All security information is placed into the NetWare server's connection list and the user is said to be logged in.

At this point, LOGIN executes one or more login scripts (which initialize environment variables, map network drives, etc.).

Related utility: LOGIN in *Utilities Reference* .

See also “LOGIN directory” ; “Login restrictions” ; “Logout” ; “Login scripts.”

LOGIN directory

The SYS:LOGIN directory, created during network installation that contains the LOGIN and NLIST utilities. Users can use these utilities to log in and view a list of available NetWare servers.

Don't delete the LOGIN directory.

See also "File system" ; "MAIL directory" ; "PUBLIC directory" ; "SYSTEM directory."

Login restrictions

Limitations on user accounts that control access to the network, such as

- **Requiring a password** If you require a password, you can specify its minimum length, whether it must be changed (and how often), whether it must be unique, and whether the user can change it.

  You can also specify the number of times a user can log in using an expired password and the number of incorrect login attempts allowed.

- **Setting account limits** If you install Accounting, you can assign account limits, like an account balance or expiration date.

- **Limiting disk space** You can limit the amount of disk space for each user by specifying the maximum blocks available for each user on a volume.

- **Specifying the number of connections** You can limit the number of times a user can log in simultaneously. You can also specify, by node address, which workstations users can log in on.

- **Setting 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.

When a user violates login restrictions, NetWare disables the account and no one can log in using that username. This prevents unauthorized users from logging in.

Related utilities: NETADMIN and NetWare Administrator in *Utilities Reference* .

Login scripts

Files containing commands that set up users' workstation environments whenever they log in. Login scripts are similar to batch files and are executed by the LOGIN utility.

You can use login scripts to

- Map drives and search drives to directories
- Display messages
- Set environment variables
- Execute programs or menus

Login scripts work the same way for DOS and Windows workstations.

Three Types of Login Scripts

When a user logs in, the LOGIN utility executes the appropriate login scripts. Three types of login scripts can be used together to specify a custom environment for your users. All three types of login scripts are optional.

- **Container login scripts** Set general environments for all users in a container (such as an Organizational Unit). These login scripts execute first.
- **Profile login scripts** Set environments for multiple users. These login scripts execute after a container login script.
- **User login scripts** Set environments specific to a single user, such as menu options or a username for electronic mail. These login scripts execute after container and profile login scripts.

The LOGIN utility contains a default login script. This login script executes the first time you log in as User object ADMIN. It contains only essential commands, such as a drive mapping to NetWare utilities.

This default login script also executes for any user who doesn't have an individual user login script.

If you don't want to create a user login script and you want to prevent the default login script from executing, you can disable the default script by including the NO_DEFAULT command in the container or profile login scripts.

Which Types of Login Scripts to Create

Maintaining many user login scripts can be time consuming. Therefore, include as much customizing information as possible in the container and profile login scripts, which are fewer in number and easier to maintain.

For example, if all users need access to NetWare utilities in the same volume, put the search drive mapping to that volume in a single container login script rather than in every user login script.

Create profile login scripts if there are multiple users with identical login script needs. These are sometimes thought of as group login scripts.

Finally, in user login scripts, include only those individual items that can't be included in profile or container login scripts.

Since up to three login scripts can execute whenever a user logs in, conflicts can occur. If this happens, the last login script to execute (usually the user login script) overrides any conflicting commands in a previous login script.

Login scripts are properties of objects.

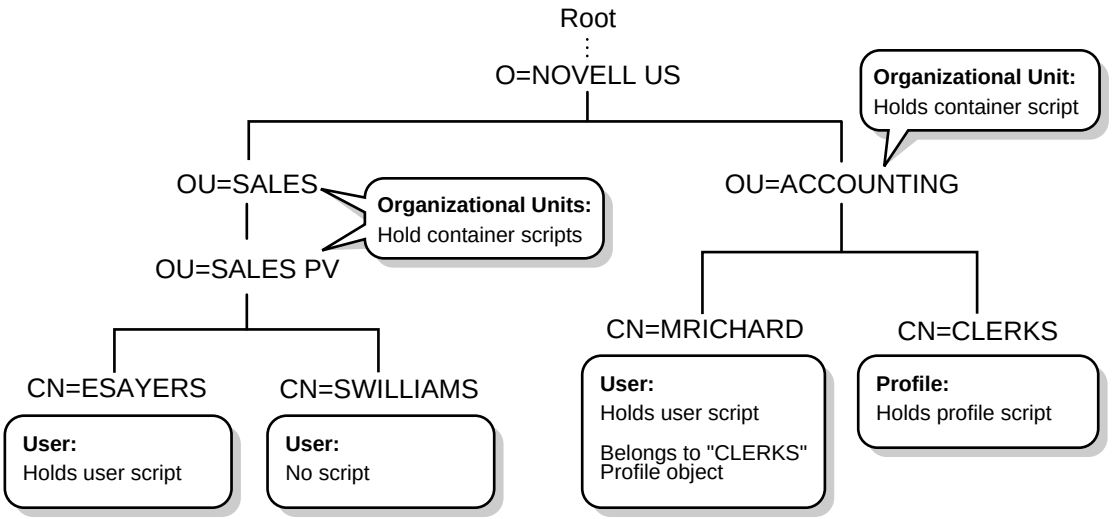
The following table shows which objects can contain login scripts

Object	Type of login script
Organization	Container
Organizational Unit	Container
Profile	Profile
User	User

The following figure shows how the different types of login scripts can reside in a Directory tree and how they affect users.

Figure 11-1

Where Login Scripts Are Located



In the previous figure, there are three users, ESAYERS, SWILLIAMS, and MRICHARD. The following table shows which login scripts execute when each user logs in.

When this users logs in	Login scripts execute in this order
ESAYERS	
	1. SALES PV's container login script
	2. ESAYERS's user login script
SWILLIAMS	
	1. SALES PV's container login script
	2. Default user login script
MRICHARD	
	1. ACCOUNTING's container login script
	2. CLERKS' profile login scriptMRICHARD's user login script

Container login scripts only affect users immediately below the Organization or Organizational Unit that contains the login script.

For example, in the figure, although there are two levels of container objects above users ESAYERS and SWILLIAMS, only the container login script immediately above them (at OU=SALES PV) executes when they log in.

If SALES PV had no container login script defined, no container login script would execute for ESAYERS and SWILLIAMS, even though a container login script exists at a higher level.

Since SWILLIAMS has no user login script defined, the default login script executes after the container login script.

Since MRICHARD belongs to the profile CLERKS, the CLERKS' profile login script executes before MRICHARD's user login script. Users can belong to only one Profile, so only one profile login script can execute for any user.

Creating, Modifying, and Copying Login Scripts

You can use either the NETADMIN utility or the NetWare Administrator utility to create or modify login scripts.

The main difference in creating container, profile, and user login scripts is the object you select to contain the scripts.

- Container login scripts are assigned to container objects (Organization or Organizational Unit objects).
- Profile login scripts are assigned to Profile objects. For a User object to use a profile login script, you must select that User object and assign it to the Profile object.
- User login scripts are assigned to User objects.

Note

A user can have login scripts in both the Directory tree and the bindery. However, if a change is made in one, that change is not automatically made in the other. You must manually edit both login scripts if you want them to be identical.

All three scripts use the same conventions, commands, and variables.

Login Script Commands

Some of the commands you can use in login scripts are listed in the following table. (For a list of all login script commands and a complete description of each, see Login Script Commands and Variables in *Supervising the Network* .)

Table 11-1 Selected Login Script Commands

Login script command	Description
ATTACH	Connects to bindery-based NetWare servers (NetWare 2 or NetWare 3) or to NetWare 4 servers using bindery services.
COMSPEC	If users run DOS from the network, this specifies the directory where the DOS command processor (COMMAND.COM) is loaded.
EXIT	Terminates execution of the LOGIN utility and executes an external program.
FIRE PHASERS	Emits a *phaser* sound when certain conditions exist.
IF...THEN	Performs an action only under certain conditions.
MAP	Maps drives and search drives to network directories and NDS objects.
PAUSE	Creates a pause in the execution of the login script.
SET	Sets a DOS environment variable.
WRITE	Displays messages on the workstation screen when a user logs in.

Identifier Variables

With many login script commands, you can take advantage of identifier variables to make your login script more efficient and flexible.

Identifier variables allow you to enter a variable (such as LOGIN_NAME) in a login script command, rather than a specific name (such as RICHARD). By using the variable, you can make the login script command applicable to many users.

When the login script executes, it substitutes real values for the identifier variables. Therefore, when Richard logs in, the command

WRITE Hello,;LOGIN_NAME

displays the following message on Richard's workstation screen:

Hello, Richard

In the above example, when Richard logged in, the name he entered was substituted for the LOGIN_NAME variable.

The following table lists identifier variables you can use in login scripts.

Table 11-2 Identifier Variables

Category	Identifier variable	Function
Date	DAY	Day number (01 through 31).
	DAY_OF_WEEK	Day of week (Monday, Tuesday, etc.).
	MONTH	Month number (01 through 12).
	MONTH_NAME	Month name (January, February, etc.).
	NDAY_OF_WEEK	Weekday number (1 through 7, with 1=Sunday).
	SHORT_YEAR	Last two digits of year (93, 94, 95, etc.).
	YEAR	All four digits of year (1993, 1994, 1995, etc.).
Time	AM_PM	Day or night (am or pm).
	GREETING_TIME	Time of day (morning, afternoon, or evening).
	HOUR	Hour (12-hour scale; 1 through 12).
	HOUR24	Hour (24-hour scale; 00 through 23, 00=midnight).
	MINUTE	Minute (00 through 59).
	SECOND	Second (00 through 59).
DOS Environment	<*variable* >	Any DOS environment variable can be used in angle brackets (<*path*> , etc.). To use a DOS environment variable in a MAP command, add a percent sign (%) in front of the variable, such as MAP S16:=%<*path*> .
Network	FILE_SERVER	NetWare server name.
	NETWORK_ADDRESS	Network number of the cabling system (8-digit hexadecimal number).
User	FULL_NAME	User's complete name in the Directory context, or full name in bindery-based NetWare.
	LAST_NAME	User's last name (surname) in NDS, or full name in bindery-based NetWare.
	LOGIN_NAME	User's unique login name. (Long names are truncated to eight characters.)

Category	Identifier variable	Function
	MEMBER OF *group*	Group object that the user is assigned to.
	NOT MEMBER OF *group*	Group object that the user isn't assigned to.
	PASSWORD_EXPIRES	Number of days before password expires.
	PLATFORM	Workstation's operating system platform: DOS, WIN (Windows3.1), WNT (WindowsNT*), or W95 (Windows95/98*)
	USER_ID	Number assigned to each user.
Workstation	MACHINE	Type of computer (IBM_PC, etc.). See your DOS manual for more information.
	OS	Type of DOS on the workstation (DRDOS, MSDOS, etc.).
	OS_VERSION	Version of DOS on the workstation (3.30, etc.).
	P_STATION	Workstation's node address (12-digit hex).
	SHELL_TYPE	Version of the workstation's DOS shell (1.02, etc.). Supports NetWare 2 and NetWare 3 shells and NetWare 4 Requester for DOS.
	SMACHINE	Short machine name (IBM, etc.).
	STATION	Workstation's connection number.
Miscellaneous	ACCESS_SERVER	Shows whether the access server is functional (TRUE=functional, FALSE=not functional).
	ERROR_LEVEL	An error number (0=No errors).
	%*n*	Replaced by parameters the user enters at the command line with the LOGIN utility.
Object properties	*property name*	You can use any property of NDS objects as a variable. Use the property's name just as you do any other identifier variable. If the property name includes a space, enclose the name in quotation marks.

Sample Login Scripts

The following sample login scripts may help you plan your own container, profile, and user login scripts. Each example script is shown in a table. The left column shows the commands in the script. The right column explains the command.

Container login script Should contain any information that applies to all users.

Table 11-3 Sample Container Login Script

Login script commands	Purpose
MAP DISPLAY OFF	Prevents map commands from displaying on the screen.
MAP ERRORS OFF	Prevents mapping errors from displaying on the screen.
MAP *1:=SYS:	Maps the first drive to volume SYS:.
MAP *1:=SYS:%LOGIN_NAME	Maps the first drive to the user's home directory. If the user has no home directory, the first drive is still mapped to SYS:.
IF %1= ADMINTHEN MAP *1:=SYS:SYSTEM	If the login name is ADMIN, it maps the first drive to SYS:SYSTEM instead of to the user's home directory.
MAP P:=SYS:PUBLIC ELSE MAP INS S1:=SYS:PUBLIC MAP INS S2:=SYS:PUBLIC\%MACHINE\%OS\%OS_VERSION END	The first search drive is mapped to SYS:PUBLIC, where DOS-based NetWare utilities are stored. The second search drive is mapped to the directory where DOS is stored. For example, if all stations use DOS, use the following two commands instead of the IF...THEN command: MAP INS S1:=SYS:PUBLIC MAP INS S2:=SYS:PUBLIC\%MACHINE\%OS\%OS_VERSION
IF MEMBER OF WIN31 THEN MAP INS *2:=SYS:USERS\%LOGIN_NAME\WIN31 MAP INS S16:=SYS:APPS\WINAPPS\WIN31 SET TEMP = P:\USERS\%LOGIN_NAME\WIN31\TEMP END	If the user who logs in is a member of Group object WIN31, the next available drive is mapped to that user's MS Windows directory. Then the next available search drive is mapped to the MS Windows directory for the WIN31 group. Finally, the MS Windows TEMP directory is set to a subdirectory of the user's MS Windows directory.
MAP INS S16:=VOL1:APPL\WP	Maps the next available search drive to the directory that contains WordPerfect*.
MAP INS S16:=VOL1:APPL\LOTUS	Maps the next available search drive to the directory that contains Lotus*.

Login script commands	Purpose
MAP INS S16:=SYS:EMAIL	Maps the next available search drive to the E-mail directory.
MAP O:=SYS:DOC	Maps drive O: to a directory necessary for running the electronic NetWare documentation.
IF MEMBER OF MANAGERS THEN MAP *3:=VOL1:PROJECTS\REPORTS END	If the user belongs to the MANAGERS Group object, the script maps the third network drive to the REPORTS directory.
IF MEMBER OF TESTERS THEN MAP *4:=INPUT:STATUS\UPDATES END	If the user belongs to the TESTERS Group object, the script maps the fourth network drive to the UPDATES directory.
COMSPEC = S2:COMMAND.COM	Sets COMSPEC to the DOS command processor, located in the DOS directory (in the second search drive).
SET PROMPT = PG	Sets the prompt to display the user's current directory path, followed by the > symbol.
MAP DISPLAY ON	Allows map commands to display.
MAP	Displays a list of all drive mappings.
WRITE	Displays a blank line between the list of mappings and following lines.
WRITE Good %GREETING_TIME, %FULL_NAME.	Displays a greeting to the user. Example: Good morning, MARY.SALES.NOVELL.
WRITE Your password expires in %PASSWORD_EXPIRES days.	Displays a message indicating the number of days before the user's password expires.
FIRE PHASERS 3 TIMES	Makes the phaser sound occur three times, to tell the user that the login process is complete.

Profile login script If you have groups of users with identical login script needs, you can create a Profile object and create a login script for the Profile object. Then, you can assign each user a member of that Profile object.

The following is an example of a profile login script you might create for users in the ACCOUNTING Profile object. The ACCOUNTING profile login script would execute after the container login script.

Table 11-4 Sample Profile Login Script

Login script commands	Purpose
MAP DISPLAY OFF	Prevents map commands from displaying on the screen as they are assigned.
MAP ERRORS OFF	Prevents mapping errors from displaying on the screen.
MAP INS S16:=VOL1:APPL\DB	Maps the first available search drive (after those assigned in the container login script) to the directory that contains the database program.
MAP *5:=VOL1:ACCOUNTS\NEW	Maps the fifth network drive (after those assigned in the container login script) to the NEW subdirectory.
MAP *6:=VOL1:ACCOUNTS\RECORDS	Maps the sixth network drive (after those assigned in the container login script) to the RECORDS subdirectory.
#WSUPDATE S1:IPXODI.COM /LOCAL	Executes WSUPDATE, which updates the IPXODI.COM file on the user's workstation with a new version of the file located in the first search drive.
MAP DISPLAY ON	Allows map commands to display.
MAP	Displays a list of all drive mappings.
WRITE	Displays a blank line between the list of mappings and following lines.
IF DAY_OF_WEEK = FRIDAY THEN WRITE Weekly progress report is due today. FIRE 2 END	On Fridays, the phaser sound occurs twice to alert the user while the message Weekly progress report is due today displays on the screen.

Login script commands	Purpose
PCCOMPATIBLE EXIT NMENU WORK	Stops the profile login script and sends the user into a menu program called WORK. EXIT also prevents user login scripts from executing. If you want a user login script to execute after the profile script, put these lines at the end of the user login script instead. DOS workstations with the machine name IBM_PC don't need the PCCOMPATIBLE line.

User login script The following is an example of a user login script for MARY. The user login script executes after container and profile login scripts.

Table 11-5 Sample User Login Script

Login script commands	Purpose
MAP DISPLAY OFF	Prevents map commands from displaying on the screen as they are assigned.
MAP ERRORS OFF	Prevents mapping errors from displaying on the screen.
MAP *7:=VOL1:MARY\PROJECTS\RESEARCH	Maps Mary's seventh network drive (after those assigned in the container and profile scripts) to the RESEARCH subdirectory in her home directory.
MAP *8:=VOL1:FORMS	Maps Mary's eighth network drive (after those assigned in the container and profile scripts) to the FORMS directory.
REM Mary needs access to FORMS while she's on the REM troubleshooting team. Remove this drive mapping REM when she's reassigned.	This remark is a reminder to the person who created the login script. It doesn't display on the user's screen. (Because the remark is several lines long, each line starts with the keyword REM.)
SET WP=/u-mjr/b-5	Sets Mary's environment variables for WordPerfect.
SET USR=mrichard	Sets Mary's user name (mrichard) for the electronic mail program.
#CAPTURE Q=FAST_Q NB TI=10 NFF	Executes the CAPTURE utility so Mary can print from non-network applications.
PCCOMPATIBLE EXIT NMENU TRAINING	Stops the user login script and sends the user into a menu program called TRAINING. DOS workstations with the machine name IBM_PC don't need the PCCOMPATIBLE line.

Note

If you did not exist as a user on a server before it was upgraded to NetWare 4 and you now need to log in via bindery services, use SYSCON (a NetWare 3 utility) to create the login script.

For information about creating, modifying, and copying login scripts, see Creating, Modifying, Copying, and Printing Login Scripts in *Supervising the Network* .

See also “Drive mapping.”

Logout

A procedure that breaks the network connection and deletes drives mapped to the network.

If you log out without specifying a NetWare server name in the LOGOUT command, the station connections and drives mapped to all servers are terminated.

To log out from one server and remain attached to the other servers, specify the server name in the LOGOUT command.

Make sure at least one of the remaining drives is mapped to the PUBLIC directory of a NetWare server that you are still attached to. Otherwise, you can't access NetWare utilities.

Related utilities: LOGOUT , NETADMIN , and NetWare Administrator in *Utilities Reference* .

Long machine type

A six-letter name representing a DOS workstation brand.

Use the long machine type in container login scripts (using the MACHINE identifier variable) to automatically map a drive to the correct version of DOS assigned to the station.

IBM computers use the long machine type IBM_PC. If the station is not an IBM computer, create a long machine type for the station in a NET.CFG file.

Use the six-letter name for the long machine type as the subdirectory name when you use more than one brand of workstation. For example, if you use COMPAQ* workstations, use COMPAQ as the long machine type.

Use the same six-letter name for DOS directories that you use for the long machine type.

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

See also “DOS version” ; “Login scripts” ; “Short machine type.”

LPT ports

The parallel printer ports of a personal computer.

See “Parallel port.”

See also Selecting the Best Type of Printer for Your Setup in *Print Services* .

LSL

(Link Support Layer) An intermediary between the NetWare server's LAN drivers and communication protocols, such as IPX, AFP, or TCP/IP.

See “Link Support Layer.”

LSP Server object

A leaf object that represents a NetWare server with the NetWare Licensing Services NLM program loaded.

When you register a License Service Provider (LSP) with Novell Directory Services, an LSP Server object is created in the same context as the NetWare Server object on which it is loaded. The LSP Server object can be moved to another context in the Directory.

See also “NetWare Licensing Services.”

Chapter 12 *M*

Mailbox ID

A unique name that specifies the directory in which all of the object's inbound mail is placed.

The utility you use to administer mailbox information (NetWare Administrator or NETADMIN) automatically assigns an object a Mailbox ID by using up to eight characters of the object's name.

However, if the object's name has spaces in it, or if it uses non-DOS characters, the utility assigns the object a Mailbox ID, but eliminates the spaces and other illegal characters to form a legal DOS name.

Mailbox location

The name of the messaging server where an object's mailbox resides.

MAIL directory

The SYS:MAIL directory, created during network installation, used by mail programs that are compatible with NetWare.

In previous versions of NetWare, the MAIL directory held user login scripts. When you upgrade to NetWare 4, existing users still have subdirectories in the MAIL directory, but their login scripts become a property of the new User object.

New users that you create under NetWare 4 won't have subdirectories in the MAIL directory.

See also "File system" ; "LOGIN directory" ; "PUBLIC directory" ; "SYSTEM directory."

Major resource

A category of data defined by the Target Service Agent, and recognized by SBACKUP.

A major resource contains data that can be backed up as a group, such as a the data on a server or volume.

See also “Backup” ; “Minor resource” ;“Target Service Agent” ; “Transaction Tracking System.”

Management Information Base

(MIB) The entire set of objects that any service or protocol uses in Simple Network Management Protocol (SNMP).

Because different network-management services are used for different types of devices or for different network-management protocols, each service has its own set of objects.

Map

For DOS clients, to assign a drive letter to a directory path on a volume.

For example, if you map drive F: to the directory SYS:ACCTS/RECEIVE, you access that directory every time you change to drive F:.

See also “Drive mapping.”

Master replica

The Directory replica used to create a new Directory partition in the Directory database or to read and update Directory information.

Although many Directory replicas can exist in the Directory, only one can be the master replica. The master replica is always considered to be the most accurate Directory replica.

See also “Novell Directory replica.”

Media Manager

A database built in NetWare that keeps track of all peripheral storage devices and media attached to NetWare servers, and allows applications to gain access and get information.

See also “NetWare Peripheral Architecture.”

Memory

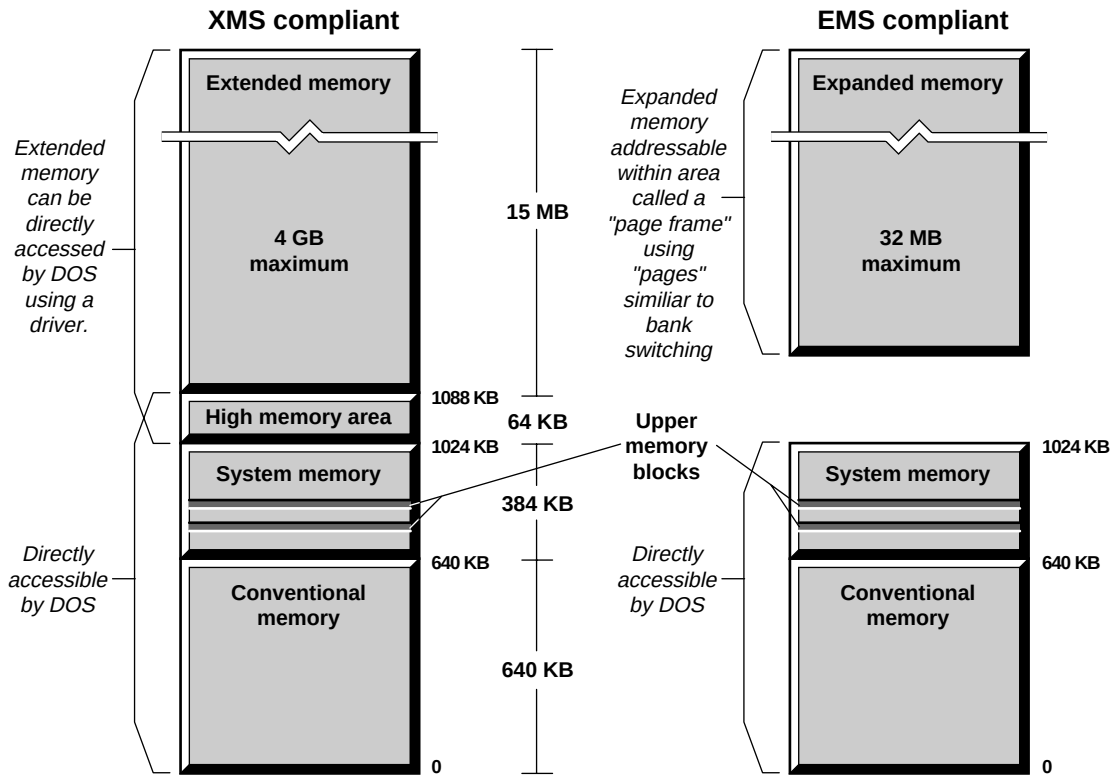
The internal dynamic storage of a computer that can be addressed by the computer's operating system, referred to frequently as RAM (random access memory).

Memory accepts and holds binary data. To be effective, a computer must store the data that is operated on, as well as the program that directs the operations to be performed.

Memory stores information and rapidly accesses any part of the information upon request.

The following figure, and the text that follows, illustrate how memory is addressed in personal computers running DOS.

Figure 12-1
Memory



Conventional Memory

RAM located below 640 KB that is devoted to running programs and applications. Also called *low DOS memory* or *base memory* .

Expanded Memory

Memory that lies outside DOS's normal address space but that can be made addressable in 16KB units, called *pages* , through an area called a *page frame* .

Expanded memory is available for 8086, 8088, and 80286 systems through expanded memory specification (EMS) compliant memory boards, or for 80386 and 80486 systems through EMS emulators.

Expanded memory is mainly designed to store data and certain numbers.

Most program code, most add-ins, and integers between –32,767 and 32,767 generally must be stored in memory that is directly addressed by DOS.

Collectively, these requirements reduce the usefulness of expanded memory.

Extended Memory

RAM above the 1,024KB address limit of DOS.

Up to 16 MB of extended memory can be addressed on 80286 systems; up to 4 GB on 80386 and 80486 systems.

Extended memory from 1,024 KB to 1,088 KB is defined as the high memory area (HMA) and can be directly addressed by DOS using drivers.

Even though extended memory above 1,088 KB can't be directly addressed by DOS or applications, DOS extenders that comply with the extended memory specification (XMS) provide access to extended memory.

Extended memory is often used for RAM disks and disk caching routines.

Upper Memory

A somewhat generic term that excludes conventional memory.

Upper memory can mean system memory (RAM between 640 KB and 1,024 KB), high memory area (RAM between 1,024 KB and 1,088 KB), extended memory (RAM above 1,024 KB) or expanded memory (also area above 1,024 KB).

High Memory Area (HMA)

The first 64 KB of extended memory from 1,024 KB to 1,088 KB. It can be directly addressed by DOS in real mode with the use of device drivers (such as HIMEM.SYS).

The high memory area provides additional memory directly addressed by DOS and functions like conventional memory.

HMA is defined in the extended memory specification (XMS), and is only available on 80286, 80386, or 80486 CPUs with more than 1,024 KB of RAM.

System Memory

The RAM between 640 KB and 1,024 KB that provides space for system use (including video adapters and other devices).

System memory isn't normally addressed by DOS or applications, but 80386 and 80486 systems can use special control programs to make upper memory blocks (UMB) in system memory that are directly addressed by DOS.

System memory is sometimes called *high DOS memory* , *high memory* , *high memory area (HMA)* , or *upper memory* .

Upper Memory Block (UMB)

A block of system memory (between 640 KB and 1,024 KB) that is directly addressed by DOS and applications.

UMBs are defined by the extended memory specification (XMS) and are created by a driver such as EMM386.EXE in DOS.

The driver converts unused address spaces in the system memory to upper memory blocks.

The upper memory blocks are then directly addressed by DOS and applications and can be loaded with applications, drivers, and terminate-and-stay-resident (TSR) programs.

Memory allocation

The process of reserving specific memory locations in RAM for processes, instructions, and data.

When a computer system is installed, the installer may allocate memory for items such as disk caches, RAM disks, extended memory, and expanded memory.

Operating systems and application programs allocate memory to meet their requirements, but they can use only that memory actually available to them.

Memory can be reallocated between resources to optimize performance. The proper memory allocation mix depends on the applications that are run.

For example, a large disk cache that speeds up one application may slow down others because there is less conventional memory available.

NetWare 4 has only one memory allocation pool, compared to NetWare 3, which has at least five allocation pools.

After continuous operation of a NetWare 3 server, applications can run out of memory because some management routines don't release memory back to the operating system.

Using one allocation pool, NetWare 4 alleviates these conditions.

Memory management routines and third-party NLM programs operate more efficiently in NetWare 4 because management operations are reduced.

NetWare 4 memory allocation routines raise the level of performance by eliminating certain conditions that often lead to inefficiencies.

Memory board

An add-on board that increases the amount of RAM within a personal computer.

See also "Memory" ; "RAM."

Message Routing Group object

A leaf object that represents a group of messaging servers that can send and receive messages among themselves.

See also "Messaging Server object."

Messaging Server object

A leaf object that represents a messaging server that resides on a NetWare server.

A Messaging Server object is automatically created in the Directory tree when you install NetWare MHS on a NetWare server. The Messaging Server object is automatically placed in the same context as the NetWare Server object.

The messaging server bundled with NetWare 4 is a NetWare Basic MHS server. It is an NLM that provides message delivery between users on a NetWare 4 LAN.

Other types of messaging servers provide different types of connectivity, or operate in different environments. For example, a Global MHSTM messaging server supports communication across asynchronous links and with non-MHS environments, such as SMTP, SNADS, and X.400.

A NetWare MHS messaging server picks up messages, which are either submitted by messaging applications (such as E-mail) or transferred from another messaging server, and delivers them to the recipients.

For recipients whose mailboxes are local on the messaging server, the message is delivered to their mailboxes. Otherwise the messaging server transfers the message to another messaging server for eventual delivery to the recipient's mailbox.

A messaging server can service an unlimited number of mailboxes. The amount of disk space available for mailboxes is the only limiting factor.

MIB

(Management Information Base) The entire set of objects that any service or protocol uses in SNMP.

See "Management Information Base."

Migrated (M) attribute

A status flag, set automatically, that indicates a file is migrated.

See also "Attributes" ; "Data migration."

Migration (operating system)

The conversion of servers from NetWare 3, or from another network operating system, to NetWare 4.

(Do not confuse migration from one version of NetWare to another with data migration, which refers to moving files to near-line or offline storage devices. See “Data migration.”)

See also “Upgrade.”

Migration (protocol)

The conversion of a server, router, or network from IPX to NetWare Link Services ProtocolTM (NLSP), or from TCP/IP to Open Shortest Path First (OSPF) protocol.

See also “IPX” ; “NetWare Link Services Protocol” ; “Open Shortest Path First.”

Minor resource

A category of data defined by the Target Service Agent and recognized by SBACKUP.

A minor resource might be located in the directory structure below the selected major resource (for example, directories, subdirectories, or files).

See also “Backup” ; “Major resource” ; “Target Service Agent” ; “Transaction Tracking System.”

Mirrored Server Engine

(MSEngine) The part of the SFT III operating system that handles nonphysical processes, such as the NetWare file system and the Directory.

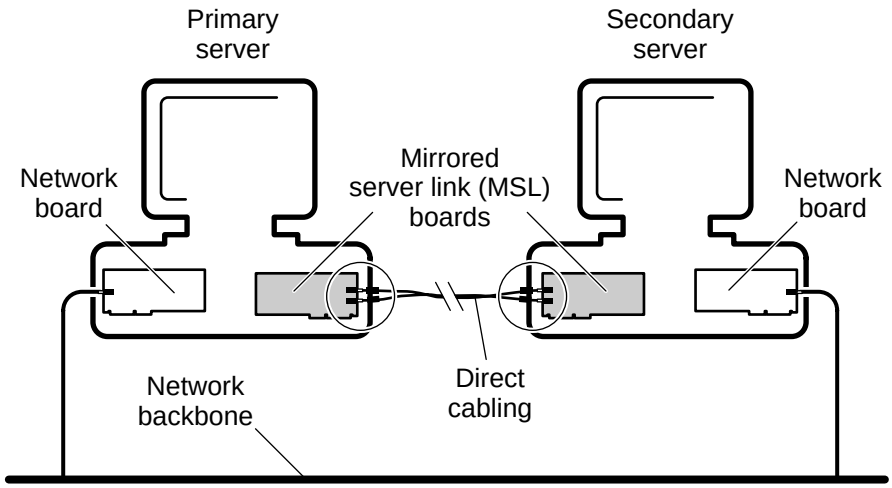
See “MSEngine.”

Mirrored server link

(MSL) A dedicated, high-speed connection between SFT III primary and secondary servers. The MSL manages server synchronization.

The MSL is essentially a bus extension from the primary IOEngine to the secondary IOEngine. It requires similar boards in each server, directly connected by fiber-optic or other cables.

Figure 12-2
Mirrored Server Link



To provide the fastest possible throughput, the mirrored server link should be a 32-bit, low latency, low CPU-utilizing board such as the NMSL board. Because of their slower speed, network boards such as the NE2000TM or the NE/2-32TM are recommended for use only as alternate MSL boards.

For system redundancy, additional MSL boards and cabling may be installed in each server. This alternate MSL connection automatically takes over (without user intervention) if the active MSL connection fails.

Mirroring

The duplication of data from the NetWare partition on one hard disk to the NetWare partition on another hard disk.

See “Disk mirroring.”

MLID

(Multiple Link Interface Driver) A device driver written to the ODI specification that handles the sending and receiving of packets to and from a physical or logical LAN medium.

See “Multiple Link Interface Driver.”

See also “Open Data-Link Interface.”

Modify bit

A file attribute set by the operating system, when a file is changed, to indicate that data has been modified.

The NetWare modify bit, called Archive Needed Attribute, appears as an A wherever file attributes are listed.

When a backup is performed, SBACKUP checks to see whether modify bits are set, and backs up only those files that have their modify bit set.

The following table shows how different types of backups handle the modify bit and process the files that aren't marked with the modify bit.

Type of backup	Modify bit setting	Treatment of non-modified files at time of next backup of this type
Full	Clear after backup	Include
Incremental	Clear after backup	Exclude
Differential	Don’t clear after backup	Exclude
Custom	As desired	As desired

See also “Backup.”

Modify right

A directory or file right that grants the right to change the attributes or name of a directory or file.

See also “Rights.”

MS Windows client

A workstation that boots with DOS and gains access to the network through either

- The requester and its programs (for NetWare 4)
- A NetWare shell (for NetWare versions earlier than NetWare 4)

The computer also runs MS Windows and, with the client software, can perform networking tasks in the MS Windows environment. These tasks include mapping drives, capturing printer ports, sending messages, and changing contexts.

See also “Client.”

MSEngine

(Mirrored Server Engine) The part of the SFT III operating system that handles nonphysical processes, such as the NetWare file system, queue management, and the Directory.

SFT III is split into two parts: the IOEngine (Input/Output Engine) and the MSEngine. The primary server and the secondary server each have a separate IOEngine, but they share the same MSEngine.

The file system, receive buffers, and queue management system all reside in the MSEngine. Applications and NLM programs that do not address hardware directly can be mirrored by loading them in the MSEngine. If one server fails, applications and NLM programs in the MSEngine continue to run.

The MSEngine keeps track of active network processes; it provides uninterrupted network service when the primary server fails and the secondary server takes over. During server switchover

- Open files stay open
- Workstation requests that have reached the receive buffers are processed without delay

Requests that have not reached the receive buffers are retried.

- Print requests that have reached the print queue remain in the queue until they can be serviced

  Requests that have not reached the queue are retried. If the print queue is assigned to a printer that is attached only to the failed server, print requests remain in the queue until the failed server is restored.

MSL

(Mirrored server link) A dedicated, high-speed connection between SFT III primary and secondary servers.

See “Mirrored server link.”

Multiple Link Interface Driver

(MLID) A device driver written to the ODI specification that handles the sending and receiving of packets to and from a physical or logical LAN medium.

See “Open Data-Link Interface.”

Multiserver network

A single network that has two or more NetWare servers operating.

On a multiserver network, users can access files from any NetWare server they have access rights to.

A multiserver network isn't the same as an internetwork, where two or more networks are linked through a router.

See also “Internetwork” ; “Network numbering.”

Chapter 13 *N*

Name context

The position of an object in the Directory tree.

See “Context.”

Name space support

Name space support is provided by NLM files that allow you to store non-DOS filenames on a NetWare 3 or 4 server. Files appear in native mode to users at different types of workstations.

Name space NLM files have a .NAM extension. (For example, MAC.NAM and LONG.NAM.)

To provide name spaces for

- **Macintosh** Load MAC.NAM.
- **OS/2, Windows 95, Windows NT** Load LONG.NAM.
- **NFS** Load NFS.NAM.
- **FTAM** Load FTAM.NAM—an add-on module you purchase separately.

To store any non-DOS file types on a NetWare volume, you must first load the name space NLM and then add the name space to the volume.

Once the name space NLM is loaded, you must use the ADD NAME SPACE console command to configure the volumes so you can store other types of file names.

You only add a name space to a volume once by using the ADD NAME SPACE command.

Note

You don't need to add a name space to a volume each time the server comes up, so the ADD NAME SPACE command does not need to be placed in your AUTOEXEC.NCF file.

Each time you mount a volume that you configured for additional name space support, (for example, each time you bring up the server), the corresponding name space module autoloads.

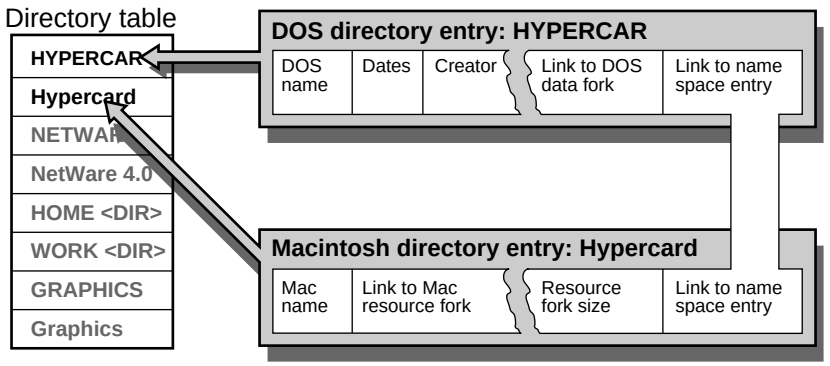
When name space support is added to a volume, another entry is created in the directory table for the directory and file naming conventions of that name space (file system).

For example, a volume that supports Macintosh files has the following for each Macintosh file:

- A DOS filename in the DOS name space
- A Macintosh filename in the Macintosh name space

These are illustrated in the following figure.

Figure 13-1
Macintosh Name Space Support



Each volume assigned to support an additional name space type requires about twice as much memory as a volume without additional name space types because the server must cache the additional directory entries.

Important

Once a name space is added to a volume, the name space can be removed from the volume only by deleting the volume and re-creating it, or by using VREPAIR . (See *Utilities Reference* .)

Name space modules (files with the *.NAM extension) should be stored with the NetWare server boot files so that you can add the additional name space to any volume, including the SYS volume.

The NetWare installation procedure places the MAC.NAM and the LONG.NAM files in the SYS:SYSTEM directory. If you purchase additional name spaces such as FTAM or NFS, consult that documentation to determine where the name space modules are placed.

Related procedure: Setting Up a Volume to Store Non-DOS Files in *Supervising the Network* .

Related utilities: ADD NAME SPACE , INSTALL , LOAD , and VREPAIR in *Utilities Reference* .

See “NetWare Loadable Module.”

Named pipes

The basis for communication between a client and advanced client-server applications such as Microsoft* SQL Server* and Microsoft Comm Server* software.

Client-server computing allows more effective use of computing resources, higher performance, greater flexibility, simpler upgrades, and, for some applications, greater reliability and data integrity.

For Novell ClientTM workstations, communication between client-server applications is implemented most frequently using the named pipes interprocess communication (IPC) protocol.

NCP

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

See “NetWare Core Protocol.”

NCP Packet Signature

An enhanced security feature that protects servers and workstations using NCPTM by preventing packet forgery.

Without NCP Packet Signature installed, a user can pose as a more privileged user and send a forged NCP request to a NetWare server.

By forging the proper NCP request packet, an intruder could gain the Supervisor object right and access to all network resources.

NCP Packet Signature prevents packet forgery by requiring the server and the user's workstation to sign each NCP packet. The packet signature changes with every packet.

NCP packets with incorrect signatures are discarded without breaking the workstation's connection to the server.

However, an alert message about the invalid packet goes out to the error log, the affected workstation, and the server console. The alert message contains the login name and the station address of the affected workstation.

If NCP Packet Signature is installed on the server and all of its workstations, it is virtually impossible to forge a valid NCP packet.

NDS

(Novell Directory Services) A relational database that is distributed across your entire network.

See "Novell Directory Services."

NetBIOS

IBM's standard protocol for applications developed to run peer-to-peer communications on the IBM PC network and the token ring network. NetBIOS has become widely accepted as a standard for network interfacing.

The Novell ClientTM for DOS and MS Windows provides a NetBIOS driver that emulates the NetBIOS protocol. This emulator allows NetWare IPX to

interface with the NetBIOS Interrupt 5Ch and an alternate interface, Interrupt 2Ah.

The NetBIOS provided by Novell is an emulator because it does not transmit NetBIOS packets. Instead, NetBIOS packets are encapsulated in IPX packets, and the IPX packets are transmitted.

The NetBIOS protocol was designed for small scale networks. While Novell has added functionality to the original specification, Novell NetBIOS emulation still works most effectively with small scale networks.

If your network contains several thousand workstations and your LAN segments are interconnected with more than one router, use SPXTM instead of NetBIOS if your applications support SPX.

NET.CFG

A workstation boot file, similar to CONFIG.SYS in DOS, that contains configuration values that are read and interpreted when your workstation starts up.

NET.CFG is created with an ASCII text editor and needs to be included on the workstation boot diskette with other boot files. NET.CFG replaces SHELL.CFG, used in earlier NetWare versions.

The configuration values in NET.CFG adjust the operating parameters of the NetWare DOS Requester, IPX, or IP protocols, and other workstation software.

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 function properly on the network.

To learn which parameters you might need to modify, consult the setup reference for each application used on your network.

Some network problems such as printing and file retrieval might also be solved by adjusting workstation parameters.

NETINFO.CFG

A NetWare server executable batch file, located on the NetWare partition of the server's hard disk.

NETINFO.CFG is used to store LOAD and BIND commands associated with protocol configuration if you used the INETCFG utility to configure the protocols.

If you have not used the INETCFG utility to configure the protocols, then the LOAD and BIND commands are placed in the AUTOEXEC.NCF file.

Some of the configuration command are written by the INETCFG utility.

Warning

Never edit this file with a text editor. Improper maintenance causes your server to malfunction.

Related utility: INETCFG in *Utilities Reference* .

See also "Router."

NetSync cluster

Includes one NetWare 4 server running NETSYNC4 and up to twelve NetWare 3.1*x* servers attached to it.

See *Installing and Using NetSync* .

NetWare Core Protocol

(NCP) Procedures that a server's NetWare operating system follows to accept and respond to workstation requests.

The process of requesting service from a NetWare server begins in the workstation's RAM where the requester requests according to the definitions of the server's NCP.

The requester then hands the requests to the station's IPX communication protocol. IPX transmits the request to the server after attaching a header designating the source and destination.

Upon receiving the request, the server removes the IPX header and reads the request.

Because the requester formed the request using the exact guidelines of a specific service protocol, the server handles the request according to the protocol rules, resulting in a proper response.

NetWare Core Protocols exist for every service a station might request from a server.

Common requests handled by NCP include creating or destroying a service connection, manipulating directories and files, opening semaphores, altering the Directory, and printing.

See also “Communication protocols” ; “IPX.”

NetWare DOS Requester

A group of files that provide NetWare support for versions of DOS and MS Windows client workstations. This requester that used VLMs is no longer supported. The NetWare DOS Requester now relies on the NET.CFG file.

NetWare Licensing Services

(NLS) A distributed, enterprise network service that lets administrators monitor and control the use of licensed applications on a network.

NLS is tightly integrated with the Novell® Directory ServicesTM (NDSTM) technology and is based on an enterprise service architecture. This architecture consists of client components that support different platforms and system components that reside on NetWare 4 servers.

NLS also provides a basic license metering tool and libraries that export licensing service functionality to developers of other licensing systems.

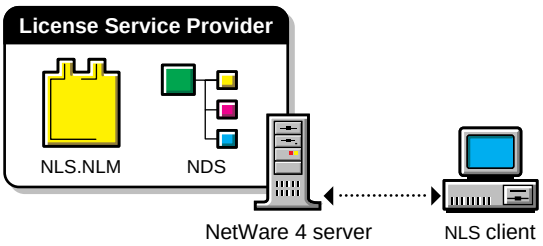
As indicated in Figure 13-2 , NLS consists of the following components:

- One or more License Service Providers (LSPs) loaded on NetWare 4 servers
- Platform-specific client components

NLS supports DOS, Windows*, Windows 95/98*, Windows NT, and NetWare 4 NLMTM clients.

- Novell Directory Services
- Transaction databases (These are not represented in Figure 13-2 .)

Figure 13-2
NLS Structure



NetWare Licensing Services client

(NLS client) Software that enables a network client to access LSAPI-compliant licensing services.

An NLS client consists of the following components:

- An application that requests services of NLS. This might be a product such as GroupWiseTM or a license usage metering utility.
- A platform-dependent licensing system software component. This is a static library\\TSR combination (in DOS) or a set of dynamic libraries (in Windows).

The client components of NLS let applications access the licensing service. There are two types of access to the licensing service that applications might require:

- Access to license certificates (objects in NDS) that conform to the industry-standard common licensing API (LSAPI). This access is necessary for applications (clients) that use the licensing service to control or monitor use.

  The components required for this type of access are platform-specific (see Table 13-1 on page 179).

- Access to administrative or management functions offered by the licensing service. This type of access is required by utilities such as NLS Manager.

NLS supports DOS, Windows 3.1x, Windows 95/98, Windows NT, and NetWare 4.2 NLM clients. The files required to support each client type are listed in Table 13-1 .

Table 13-1NLS Client Types

Client Type	Required Files
DOS	A static library file and TSR program provide license resource access for DOS clients. The appropriate static library file is used by software developers when they write a licensed application.
	NLSLSAPI.EXE. An LSAPI-compliant TSR for NetWare Licensing Services. This TSR must be loaded before the DOS client application is executed; otherwise, an error is returned for any LSAPI function.
Windows	**LSAPI.DLL.** A generic LSAPI v1.1 client component for accessing any licensing service. LSAPI.DLL reads the LICENSE.INI file and loads the appropriate client components.
	NLS.DLL and NLS32.DLL. NLS-specific client components that enable license resource access for Windows clients.
NLM	**LSAPI.NLM.** A shared library NLM that provides LSAPI v1.1 calls for NLM clients. This module should be loaded before the licensed NLM.
	NLSAPI.NLM. A shared-library NLM that provides access to NLS management functions. This module should be loaded before the licensed NLM.

NetWare Link Services Protocol

(NLSP) A link state routing protocol designed by Novell for IPX internetworks.

NLSPTM is derived from IS-IS (Intermediate System-to-Intermediate System), the link state routing protocol developed by the International

Standards Organization (ISO). Like IS-IS, NLSP transfers routing information between routers and makes routing decisions based on that information.

NLSP routers exchange link information such as network connectivity, path costs, IPX network numbers, media types, etc. By exchanging this information with its peer routers, each router builds and maintains a complete logical map of the network.

Unlike RIP and SAP, which periodically broadcast routing and service information, NLSP multicasts routing information only when a change occurs in a route or service on the network.

To communicate with Novell Clients, NLSP routers use RIP.

See also “Link state.”

NetWare Loadable Module

(NLM) A program you can load and unload from server memory while the server is running. (Some NLM programs are loaded automatically because other NLM programs can't run without them.)

When loaded, an NLM program is dynamically linked to the operating system, and the NetWare server allocates a portion of memory to it.

The amount of memory an NLM program uses depends on the task. Some tasks make calls that cause the operating system to allocate more memory.

The NLM uses the memory to perform a task, and then returns control of the memory to the operating system when the NLM is unloaded.

When an NLM is unloaded, all allocated resources are returned to the operating system.

NetWare 4 has four types of NLM programs:

- Disk drivers (.DSK extension) control communication between the operating system and hard disks.

  You can load and unload disk drivers while the server is running.

- NWPA drivers (.CDM and .HAM extensions) control communication between the operating system and host adapters.

- LAN drivers (.LAN extension) control communication between the operating system and the network boards.

  You can load and unload LAN drivers while the server is running and users are logged in.

- Management utilities and server applications modules (.NLM extension) allow you to monitor and change configuration options.

  For example, you can run VREPAIR on a dismounted volume, add disk space to a mounted volume, or surface test a disk drive while the NetWare server is running.

  Once you finish your tasks, you can unload the utility and free memory for other server functions.

- Name space support (.NAM extension) allows non-DOS naming conventions to be stored in the directory and file naming system.

Some NLM programs, such as utilities, can be loaded, used, and then unloaded. Other NLM programs, such as LAN driver and disk driver NLM programs, must be loaded every time the server is booted.

NCF files (STARTUP.NCF and AUTOEXEC.NCF) allow you to store NLM commands that you want loaded every time the NetWare server is booted.

Most NLM programs released with NetWare 4 are copied to SYS:SYSTEM during installation. As you acquire additional NLM programs, decide where you want to copy them. The operating system must be able to find the NLM programs when a LOAD command is issued.

NLM programs can be copied to any of the following areas:

- The SYS:SYSTEM directory
- Any network directory on the NetWare server
- A local drive of the NetWare server

Related utilities: LOAD , UNLOAD , and SEARCH in *Utilities Reference* .

See also “Loading and unloading.”

NetWare Management Agent

A group of NLM programs that provide server statistics and notify the ManageWise® console of alarm conditions.

When installed on each server in the network, NetWare Management Agent allows you to monitor, manage, and maintain all servers from a central console.

For example, with NetWare Management Agent software, you can

- View the configuration of a server, including NLM programs installed, printers and print queues, hard disks and disk controllers, and LAN drivers
- Monitor server traffic and server memory use
- Specify alarm settings for server errors and events

NetWare Management Agent provides a graphical representation of all managed objects and their attributes, including a server's hardware, software, or data components.

NetWare MHS Services

Services that allow users to communicate electronically across a network.

Using messaging services, users can exchange electronic mail, share calendars, schedule facilities, etc.

To provide messaging services, NetWare uses a messaging server, a Distribution List object, a Message Routing Group object, an External Entity object, and a Postmaster.

NetWare Name Service

(NNS) A naming service designed to provide more transparent access to resources in NetWare installations.

NNS was a predecessor to NDS, and consisted of a set of specialized utilities designed to work with existing NetWare 2 and NetWare 3 networks.

Using NNS, users could more easily log in to multiple file servers and print to specific print queues, and network administrators could more easily manage users and groups on multiserver networks.

NNS is no longer available or supported.

See also “Novell Directory Services.”

NetWare Networked File System

(NetWare NFS) Software that transparently integrates UNIX systems with NetWare 4 file systems and resources to give UNIX users access to the NetWare environment from their native operating system.

NetWare NFS

Software that transparently integrates UNIX systems with NetWare 4 file systems.

See “NetWare Networked File System.”

NetWare operating system

The network operating system developed by Novell, Inc. NetWare runs on the server and provides several functions to the network and the applications running on it, including

- File and record locking
- Security
- Print spooling
- Interprocess communications

The NetWare operating system also determines performance, multivendor support, and reliability of the network.

NetWare partition (disk)

A partition created on each network hard disk, from which NetWare volumes are created.

Note

NetWare disk partitions are not related to NetWare Directory partitions. Disk partitions are subdivisions of a hard disk. A Directory partition is a subtree within the Directory tree. (See “Novell Directory partition.”)

See “Disk partition.”

NetWare Peripheral Architecture

(NWPA) An extension of the NetWare 4 Media Manager (a database built into NetWare for managing storage devices and media).

NWPA provides broader and more flexible driver support for host adapters and storage devices.

NWPA separates NetWare driver support into two components: a HAM and a CDM. The HAM drives the host adapter hardware. The CDM drives storage devices or autochangers attached to a host adapter bus.

Instead of .DSK files, you can load .HAM and .CDM files when available for your adapter and devices. The integrated architecture of HAMs and CDMs may provide better performance, especially for CD-ROM drives and magneto-optical disk drives.

Loading HAMs and CDMs is much like loading other device drivers, but instead of loading one .DSK file for both the adapter and device, you load one .HAM file for the adapter and one .CDM file for each device attached to the adapter.

When you want to connect a new hardware device to the host bus adapter, you need to load only the appropriate CDM for that hardware device (in addition to the HAMs and CDMs already loaded and assuming a compatible adapter is installed).

A brief description of some NWPA components follows:

Media Manager

A database built into NetWare that keeps track of all peripheral storage devices and media attached to NetWare servers, and allows applications to gain access and get information.

The Media Manager receives application I/O requests and converts them to messages compatible with the NWPA architecture.

Host Adapter Module (HAM)

The driver component associated with the host adapter hardware. HAMs are adapter-specific. For example, if a third-party adapter is installed in the server, a HAM developed specifically for that adapter must be installed during installation of NetWare 4 custom installation (not a simplified installation).

HAMs provide the functionality to route requests to the bus where a specified device is attached.

Host Adapter Interface (HAI)

A set of APIs within the NWPA that provide an interface for HAMs to communicate with the Media Manager.

Custom Device Module (CDM)

The driver component associated with storage devices attached to the host adapter. CDMs are device-specific. For example, if there are three storage devices attached to the host adapter, a specific CDM for each device must be installed with NetWare 4 during a custom installation (not a simplified installation).

Custom Device Interface (CDI)

A set of APIs within the NWPA that provides an interface for CDMs to communicate with the Media Manager.

NetWare protocols and transports

The components of NetWare software that allow client workstations to communicate and be understood on the network.

A *protocol* manages data and a *transport* manages application messages. A protocol and transport can be provided by one piece of software or by many.

In order for client workstations to communicate on the network, they must use a protocol identical to the one used on the network. However, workstations can be configured to use multiple protocols.

The Novell Client Software provides the following standard protocols:

- Address Resolution Protocol (ARP)
- BOOTP (Provides TCP/IP configuration information)
- Internet Control Message Protocol (ICMP)
- Internet Protocol (IP)
- IPX/SPX
- Management Information Base (MIB)
- NetBIOS
- Reverse Address Resolution Protocol (RARP)
- Remote Program Load (RPL)
- System Network Architecture (SNA)
- Simple Network Management Protocol (SNMP)
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Xerox Network System (XNS)

See also “Address Resolution Protocol” ; “BOOTP” ; “Internet Control Message Protocol” ; “Internet Protocol” ; “IPX” ; “Management Information Base” ; “NetBIOS” ; “Reverse Address Resolution Protocol” ; “Remote Program Load” ; “Simple Network Management Protocol” ;“System Network Architecture” ; “Transmission Control Protocol” ; “User Datagram Protocol” ; “Utilities.”

NetWare Runtime

A single-user version of the NetWare 4 operating system that provides NetWare services to clients of NLM programs.

Benefits of a Runtime Server

NetWare RuntimeTM is a network server platform supporting front-end or back-end applications as well as basic NLM services such as communication services, database servers, electronic mail, and other third-party applications.

NLM application developers have the flexibility to determine which client services are available in their product.

NLM programs, loaded on a NetWare Runtime server, provide client connection services (using IPX, SPX, or TCP/IP).

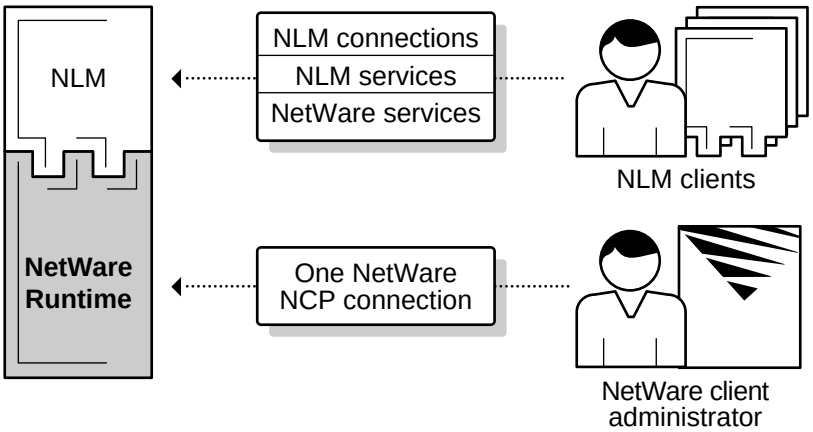
How Runtime Works

Network clients attach to the NLM that runs on top of NetWare Runtime. The NLM provides all services required by the client using NetWare application program interfaces (APIs).

Specific NetWare services are available to clients only through the NLM applications which serve those clients. The NLM program implements and manages any required client services.

The following figure shows how NetWare Runtime functions:

Figure 13-3
NetWare Runtime



For example, a database NLM application may provide a client with login connections (including authentication), file services, data access, and disconnect services.

Other NetWare services can be built into NLM applications to provide additional functionality.

Limitations of a Runtime Server

Only one user can log in to the NetWare Runtime server at a time. Normally, the network supervisor logs in for administrative purposes using the single allowed NetWare Core Protocol (NCP) connection.

Utilities That Don’t Apply to a Runtime Server

Though all NetWare 4 utilities and commands are available on a Runtime server, some don’t apply or wouldn’t be used because of the server’s single-user environment.

You aren’t likely to use the following utilities:

CAPTURE
DCONFIG
NMENU
NPRINT

PCONSOLE
PRINTCON
PRINTDEF
PSC
SEND
SETTTS
SYSTIME
WSUPDATE

In addition to utilities, you don't need several network supervisor commands, such as commands associated with creating or modifying login scripts or menus, as well as those related to workstation management.

NetWare Runtime Installation

The procedures for installing a NetWare 4 Runtime server are the same as for any NetWare 4 server.

For information on how to install a Runtime server, see *Installation and Upgrade*.

NetWare server

A computer that runs NetWare operating system software.

A NetWare server regulates communications among personal computers attached to it and to shared resources, such as printers.

A NetWare 4 server must have at least one hard disk, either internal or external, and a recommended minimum 16 MB of RAM. The server must also contain at least one network board.

NetWare servers running NetWare 4 can be used only as dedicated servers.

Related utility: INSTALL in *Utilities Reference* .

NetWare Server object

A leaf object that represents a server running NetWare on your network.

A NetWare Server object can represent a server running any version of NetWare.

Certain objects, such as Volume objects, reference a NetWare Server object to help identify their locations.

Important

Use caution when removing the Supervisor right from the Inherited Rights Filter of a NetWare Server object. You could cut off access to part of the Directory tree. (See "Inherited Rights Filter.")

See also "Object" ; Creating Leaf Objects and Cautions When Deleting NetWare Server Objects in *Supervising the NetWork* .

NetWare user tools

Software that provides you with a graphical means of accessing network resources, such as volumes, directories, printers, and users.

NetWare user tools allow you to perform tasks such as managing drive mappings, managing printer connections and setup, managing server connections, displaying network users, and sending messages.

For more information on NetWare user tools for DOS and Windows workstations, see the Novell Client documentation.

NetWare volume

A physical amount of hard disk storage space, fixed in size. A NetWare volume is the highest level in the NetWare directory structure (on the same level as a DOS root directory).

See "Volume."

NetWire

An online information service, which provides access to Novell product information, Novell services information, and time-sensitive technical information for NetWare users.

NetWire® allows you to

- Access information remotely 24 hours a day
- Submit questions to a Novell Technician or System Operator
- Download files and technical information dealing with product updates and modifications

NetWire is accessed through the CompuServe* Information Service. It requires a PC or compatible workstation, a modem, and a communications program.

Contact CompuServe for more information on NetWire subscriptions and a free introductory subscription.

- In the USA or Canada, call 1-800-524-3388.
- In all other locations, call 1-614-457-0802.

Ask for representative 200.

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 NetWare servers.

NetWare network users can share the same files (both data and program files), send messages directly between workstations, and protect files with an extensive security system.

Network address

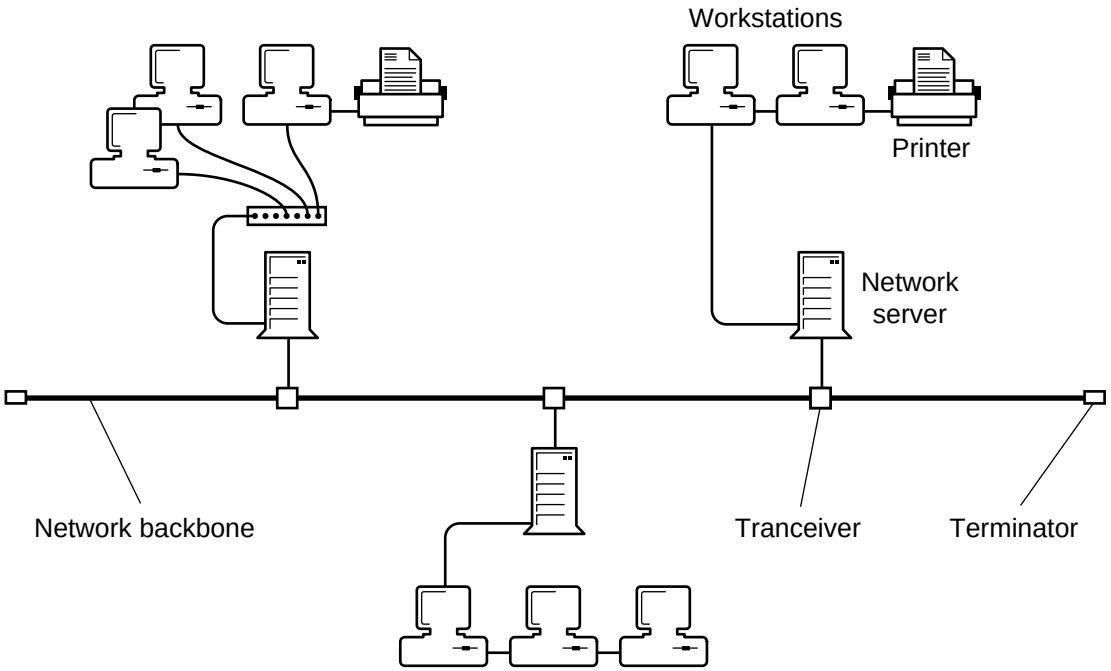
A network number that uniquely identifies a network cable segment; usually referred to as the *IPX external network number.*

See “IPX external network number.”

Network backbone

A cabling system that NetWare servers and routers are attached to. The central cable handles all network traffic, decreasing packet transmission time and traffic on the network.

Figure 13-4
Network Backbone



Network board

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

Some printers contain their own network board to allow them to attach directly to the network cabling.

NetWare documentation uses the term *network board* . Documentation from other companies might use the terms *NIC* or *network card* instead of *network board* .

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 direct printer

Printers and third-party print queue servers that connect directly into the network.

In many cases, these devices (direct-connect printers and queue servers) offer an effective printing solution in NetWare printing environments.

Typically, these print devices are shipped with their own installation utilities. The manufacturer's utilities configure the device to recognize network print components and to communicate with the network.

Many network-direct print devices and their installation programs are designed to search the NetWare 3 bindery for network printing information. In order for these devices to work on a NetWare 4 network, you should use the bindery services mode when installing them.

See also Using Third-Party Network-Direct Print Devices with NetWare 4 in *Print Services* .

Network drive

A common name for a *logical drive* .

See "Drive."

Network node

A personal computer or other device connected to a network by a network board and a LAN driver.

A network node can be a server, workstation, router, printer, or fax machine.

Network number

A number that uniquely identifies a network cable segment, usually referred to as the *IPX external network number.*

See “IPX external network number.”

Network numbering

The system of numbers that identifies servers, network boards, and cable segments. These network numbers include the following:

- **IPX external network number** is a number that identifies a network cable segment.

  Servers that use the same frame type must use the same external network number to identify a specific cable segment.

  For example, all servers using frame type 802.2 could identify a particular cable segment as AAAAAAAA. If a new server using the same frame type is added to the network, it must also refer to this cable segment as AAAAAAAA.

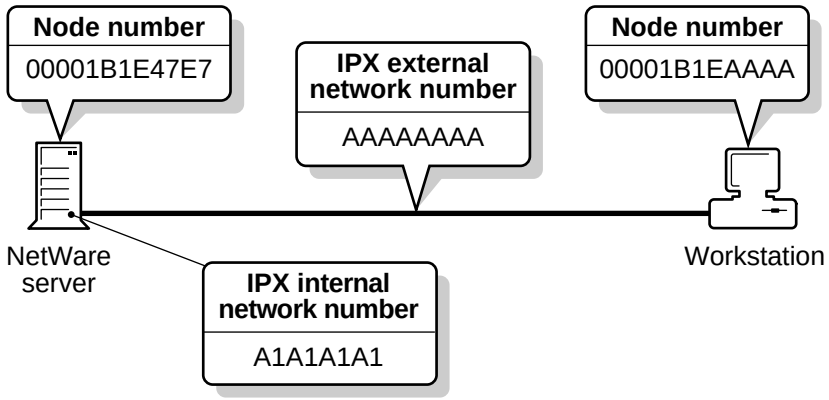
  On the other hand, if a server with a different frame type is added to the network, it must use a different external network number for the same cable segment. It must use the same external network number as other servers of its frame type.

- **IPX internal network number** is a number that identifies an individual NetWare 4 server. This number must be unique for each server.

- **Node number** is a number that identifies a network board (in a server, workstation, or router). This number must be unique for each board.

The relationship of these numbers is illustrated in the following figure.

Figure 13-5
NetWork Numbering



See also “IPX external network number” ; “IPX internal network number” ; “Node number.”

Network printer

A printer shared in a network environment.

See also “Printer” ; Setting Up Printers Attached to Workstations or Servers in *Print Services* .

Network supervisor

A generic term in NetWare 4 for the person responsible for configuring the NetWare server, workstations, user access (security), printing, etc.

Network Support Encyclopedia Professional Volume

(NSE ProTM) An electronic information database containing comprehensive information about network technology.

The Network Support Encyclopedia Professional VolumeTM includes Novell technical bulletins and manuals, as well as downloadable NetWare patches, fixes, drivers, and utilities.

NSE Pro℠ contains NetWare Application NotesTM(with graphics), the NetWare Buyer's Guide, Novell press releases, and additional product information.

The NSE Pro also includes Novell LabsTM hardware and software compatibility test results.

Using the text-retrieval software included with the NSE, you can search through custom menus, browse through manuals and technical bulletins, and do string searches using Boolean logic.

The NSE Pro is available on CD-ROM in one year subscription which includes updates.

For more information on subscribing to the NSE Pro, contact your Novell Authorized Reseller℠ .

NFS

Networked file system. NetWare® NFS* allows UNIX systems to integrate with NetWare 4 file systems.

See "NetWare Networked File System."

NIC

(Network interface card) A circuit board installed in each workstation to allow stations to communicate with each other and with the NetWare server.

NetWare documentation uses the term *network board* instead of *NIC* .

NLM

(NetWare Loadable Module) A program you can load and unload from server memory while the server is running.

See "NetWare Loadable Module."

NLSP

(NetWare Link Services Protocol) A link-state routing protocol designed by Novell for IPX internetworks.

See “NetWare Link Services Protocol.”

NNS

(NetWare Name Service) A naming service designed to provide more transparent access to resources in NetWare installations. NNS was a predecessor to NDS.

See “NetWare Name Service.”

See also “Novell Directory Services.”

Node address

A number that uniquely identifies a network board; usually referred to as the *node number* .

See “Node number.”

Node number

A number that uniquely identifies a network board, also known as *station address*, *physical node address*, and *node address.*

Every node must have at least one network board, by which the node is connected to the network. Each network board must have a unique node number to distinguish it from all other network boards on that network.

Node numbers are assigned in several ways, depending on the network board type:

- Ethernet and token ring boards are factory-set (with no two Ethernet boards having the same number).
- ARCnet* board numbers are set with jumpers or switches.

See also “IPX internetwork address.”

Normal (N) attribute

A file system attribute that indicates that no NetWare attributes are set.

See also “Attributes.”

Novell Directory database

The database (commonly referred to as *the Directory*) that organizes Novell Directory Services objects in a hierarchical tree structure called the *Directory tree* .

See “Novell Directory Services.”

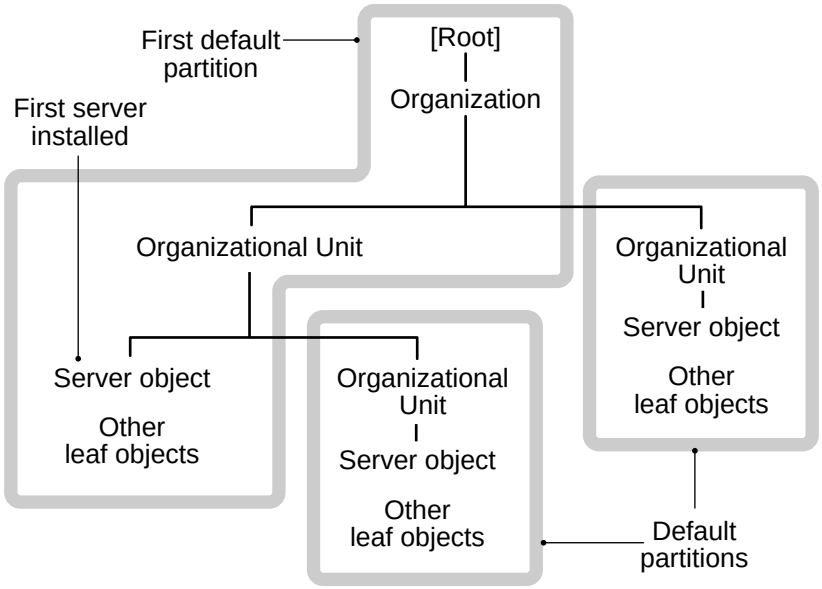
Novell Directory partition

A logical division of the Novell Directory database. A Directory partition forms a distinct unit of data in the Directory tree that you use to store and replicate Directory information.

Each Directory partition consists of a container object, all objects contained in it, and data about those objects. Directory partitions don't include any information about the file system or the directories and files contained there.

The following figure shows the default Directory partition created for the first server installed and for all the new Organizational Units in which NetWare 4 servers were installed.

Figure 13-6
Example of Default Directory Partitions



Under NDS, an object resides in only one Directory partition, but through distributed operations, the object can be accessed from any point on the network.

To optimize access to different areas of the Directory, each Directory partition can be replicated and stored at many locations.

Directory partition replication improves access to Directory information and provides the Directory with fault tolerance. Since a Directory partition can be replicated at several locations, damage to one of the Directory replicas doesn't need to interrupt access to partition information.

Furthermore, the Directory allows Directory replicas to be designated as read/write or read-only, thus controlling the introduction of updates into the system.

The tree of Directory partitions is transparent to Directory users (unless they are running the NDS Manager utility; users usually see only a global tree of Directory objects.

Replicas of Directory partitions are stored on NetWare servers. Multiple replicas of different Directory partitions can be stored on the same NetWare server; none of the Directory partitions need to be contiguous to each other.

See also “Novell Directory Services” ; “Novell Directory replica” ; Managing the Novell Directory Tree in *Supervising the Network* .

Novell Directory replica

A copy of a Novell Directory partition.

For the Directory database to be distributed across a network, it must be stored on many servers. Rather than storing a copy of the whole Directory database on each server, Directory replicas of each Directory partition are stored on many servers throughout the network.

You can create an unlimited number of Directory replicas for each Directory partition and store them on any server.

Purpose of Directory Replicas

Directory replicas serve two purposes:

- To eliminate any single point of failure

  For example, if a disk crashes or a server goes down, a Directory replica on another server can still authenticate users to use the network and can provide information on objects in that Directory partition.

  With the same information distributed on several servers, you aren't dependent on any single server to authenticate who can use the network.

  You can store a Directory replica of one Directory partition with a Directory replica of another Directory partition on the same server.

Important

Replication of the Directory doesn’t provide fault tolerance for your file system. Only Directory information about objects is replicated. To provide fault tolerance for your files, you must mirror or duplex your hard disks and be sure TTS is enabled. (See “Disk duplexing” ; “Disk mirroring” ; “Transaction Tracking System.”)

- To provide faster access to information for users across a WAN link

  For example, if a WAN link is used to access information, you can decrease access time and network traffic by placing a Directory replica containing the needed information on a server that users can access locally.

Distributing Directory replicas among servers lets you access information more quickly and reliably because the information comes from the nearest available server.

Types of Directory replicas

- **Master replica** Although many Directory replicas can exist in the Directory, only one is the master replica. Use it to create a new Directory partition in the Directory database, or to read and update Directory information, such as adding or deleting objects.
- **Read/write replica** Use to read or update Directory information (such as adding or deleting objects).
- **Read-only replica** Use to view, but not to modify, Directory information.
- **Subordinate reference replica** You cannot modify this type of Directory replica. NDS automatically places a subordinate replica on the server if the parent Directory partition has either a master, read/write, or read-only replica on the server and the child Directory partition does not.

  If you add a read/write or read-only replica of the child Directory partition to the server, the subordinate replica disappears.

Synchronization of Directory replicas

To maintain its fault tolerance, the replicas of a Directory partition are periodically (and automatically) updated, or *synchronized* .

When changes are made in one Directory replica, synchronization ensures that those changes are made in all other Directory replicas of that partition, so that each Directory partition's replica contains the same data as the other Directory replicas.

Network supervisors cannot control how often Directory replica synchronization occurs; NDS handles Directory replica synchronization automatically. But, supervisors can manually synchronize Directory replicas using NDS Manager.

For more information, see NDS Manager in *Utilities Reference* .

See also “Novell Directory partition” ; Maintaining NetWare 4 Networks in *Supervising the Network* .

Novell Directory Services

(NDS) A relational database that is distributed across your entire network. NDS provides you with global access to all network resources to which you have been given rights, regardless of where they are physically located.

NDS treats all network resources as objects in a distributed database known as the *Novell Directory database* , also referred to as the *Directory.*

All users log in to a multiserver network and view the entire network as a single information system. This single view provides for increased productivity and reduced administrative costs.

Note

NDS helps you manage Directory resources such as NetWare servers and volumes, but it doesn’t provide control over the file system (files and file directories). Graphical and text utilities are available that help you control the file system.

Authentication

When a user accesses resources on the network, background authentication processes verify that the user has rights to use those resources.

Authentication allows users (who have logged in) to access any server, volume, or printer to which they have rights. User trustee rights restrict the user's access within the network. (See also “Authentication” ; “Login scripts” ; “Rights” ; “Trustee.”)

Objects

Within NDS, objects represent network resources. An object consists of categories of information, called *properties* , and the data in those properties. The information is stored in the Novell Directory database.

Some objects represent physical entities. For example, a User object represents a user and a Printer object represents a printer.

Some objects represent logical entities, such as groups and print queues.

Other objects, such as the Organizational Unit object, help you organize and manage objects. (See “Object.”)

The Directory Tree

NDS operates in a logical organization called the Directory tree. It is called a Directory tree because objects are stored in a hierarchical tree structure, starting with a root object and branching out. (See “Directory tree.”)

Directory Partitions

To make it more manageable, the Novell Directory database is divided into smaller portions called *Directory partitions* . Directory partitions are created by default when you install NetWare 4 on a server in a new context in the Directory tree. (See “Novell Directory partition.”)

Directory Replicas

For NDS to be distributed across a network, the Directory database must be stored on many servers. Rather than have a copy of the whole Directory database on each server, *Directory replicas* of each Directory partition are stored on many servers throughout the network.

Directory partition replication improves access and provides the Directory with fault tolerance. Since a Directory partition can be replicated at several locations, damage to one of the Directory replicas doesn't need to interrupt access to the Directory partition information. (See “Novell Directory replica.”)

Time Synchronization

Time synchronization establishes the order of events in NDS.

Whenever an event occurs in the Directory, such as a password changed or an object renamed, NDS requests a *time stamp* so that the Directory replicas are updated in the correct order. (See “Time synchronization.”)

Bindery Compatibility

NDS replaces the bindery, which served as the system database in earlier versions of NetWare. To provide compatibility with earlier, bindery-based

versions of NetWare that may co-exist with NDS on the network, NetWare 4 features bindery services. (See “Bindery services.”)

Novell Directory Services management request

A request that controls the physical distribution of the Directory database. Through these requests, system administrators can create new Directory partitions and manage their Directory replicas.

The following requests are supported:

Request	Description
Add replica	Adds a Directory replica of an existing Directory partition to a server.
Delete replica	Deletes a Directory replica from a server.
List replicas	Lists the Directory replicas stored by a server.
Change replica type	Changes Directory replica type to master, read/ write, or read-only.
Send updates to other replicas	Sends updated information from the current master replica to all replicas of the Directory partition.
Receive updates from other replicas	Updates the current master replica with information from all the replicas of the Directory partition.
Create a new partition	Splits a Directory partition into two at a specified object.
Merge partition	Joins the Directory partition at the specified objects.
Abort partition operation	Aborts the creating of a new Directory partition or the merging of a Directory partition.

See also “Novell Directory partition” ; “Novell Directory replica.”

NWPA

(NetWare Peripheral Architecture) An extension of the NetWare 4 Media Manager that separates NetWare driver support into two components; a HAM

for the host adapter hardware, and a CDM for devices attached to the host adapter.

See “NetWare Peripheral Architecture.”

NSE Pro

(NetWare Support Encyclopedia Professional Volume) A Novell database that contains comprehensive information about network technology.

See “Network Support Encyclopedia Professional Volume.”

Chapter 14 O

Object

An NDS structure that stores information about a network resource (such as a user, group, printer, or volume).

An object consists of categories of information, called *properties* , and the data in those properties. The information is stored in the Novell Directory database.

Some objects represent physical entities. For example, a User object represents a user and a Printer object represents a printer.

Some objects represent logical entities, such as groups and print queues. Other objects, such as the Organizational Unit object, help you organize and manage objects.

Remember that an object is a structure where *information* about the entity is stored; it isn't the actual entity.

For example, a Printer object stores information about a printer and helps manage how the printer is used, but it isn't the printer itself.

Types of Objects

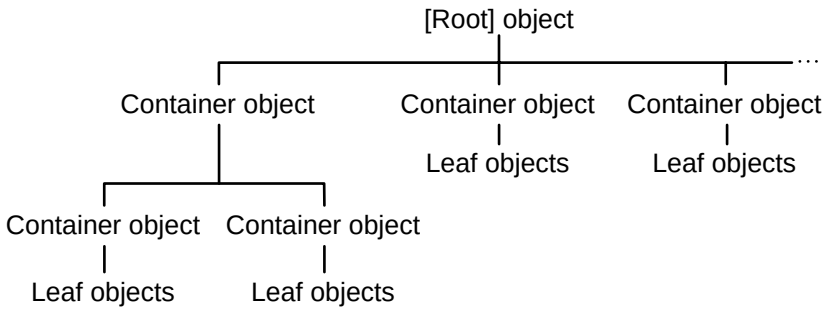
Two types of objects make up the Directory tree: *container objects* and *leaf objects* .

A subtree, or branch, of the Directory tree consists of a container object and all the objects it holds, which can include other container objects.

Leaf objects are at the ends of branches and don't contain other objects.

The following figure shows how container objects and leaf objects make up the Directory tree.

Figure 14-1
Objects in a Directory Tree



Container objects hold, or contain, other objects. Container objects are used as a way to logically organize all other objects in the Directory tree.

The [Root] object is also considered a container object, but it is the very first object in the Directory tree, and it cannot be deleted or modified. All other objects, including Organization objects, are contained within the [Root] object.

Container objects are like directories in a file system in that they group related information together. If a container object has objects in it, it is called a parent object.

Types of container objects. There are three types of container objects, described in the following table:

Table 14-1 Types of Container Objects

Container object	Abbreviation	Description
Country	C	Designates the countries where your network resides and organizes other Directory objects within the country. (See “Country object.”)
Licensed Product	LP	The Licensed Product container object is created automatically when you install a license certificate or create a metering certificate using NetWare Licensing Services (NLS) technology.When an NLS-enabled application is installed, it should add a Licensed Product container object to the Novell Directory database and a License Certificate leaf object to that container.
Organization	O	A level below the Country object (unless you don't use the Country object), the Organization object helps you organize other objects in the Directory and allows you to set template information for users created in this container. (See “Organization object.”)
Organizational Unit	OU	A level below the Organization object, the Organizational Unit object helps you to further organize other objects in the Directory and also allows you to set template information for users created in this container. (See“Organizational Unit object.”)

Country objects can contain Organization objects or Alias objects (a leaf object, described in the next section).

Organization and Organizational Unit objects can contain Organizational Unit objects or leaf objects.

Types of leaf objects. Leaf objects don’t contain other objects. They represent network resources, such as users, computers, printers, and lists. The following table describes leaf objects:

Table 14-2 Types of Leaf Objects

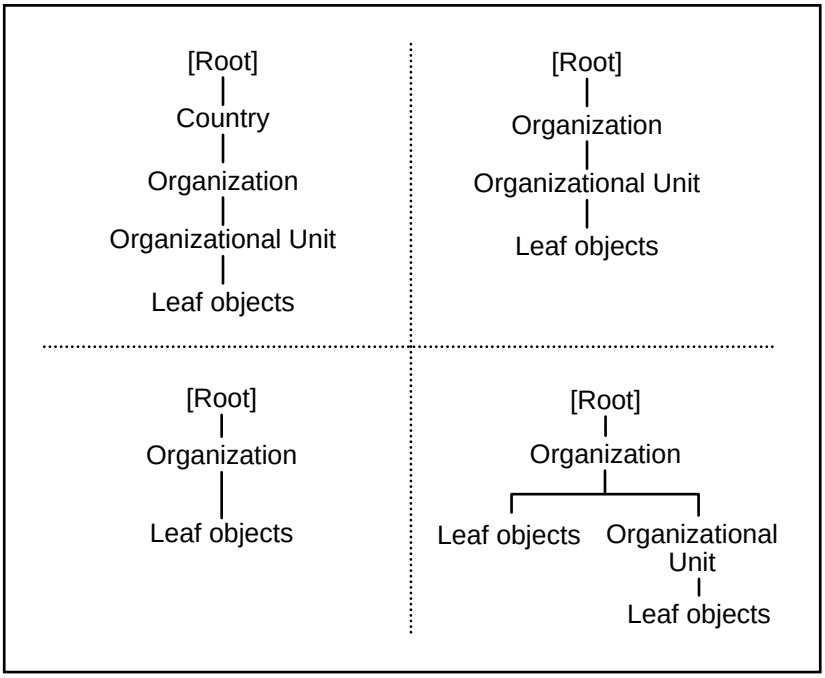
Leaf object	Description
Alias	Points to the original location of an object in the Directory. Any Directory object located in one place in the Directory can also appear to be in another place in the Directory by using an Alias. (See “Alias object.”)
Application	Represents a network application. Application objects simplify administrative tasks such as assigning rights, customizing login scripts, and supporting applications.
Auditing File	The Novell Directory Services data structure used to manage an audit trail's configuration and access rights.
Bindery	Represents an object placed in the Directory tree by an upgrade or migration utility, but that NDS can't identify. This object provides backward compatibility for bindery-oriented utilities. (See “Bindery object.”)
Bindery Queue	Represents a queue placed in the Directory tree by an upgrade or migration utility, but that NDS can't identify. This object provides backward compatibility for bindery-oriented utilities.
Computer	Represents a computer on the network. (See “Computer object.”)
Directory Map	Refers to a directory on a volume. (See “Directory Map object.”)
Distribution List	Represents a list of mail recipients. (See “Distribution List object.”)
External Entity	Represents a non-native NDS object that is imported into NDS or registered in NDS. (See “External Entity object.”)
Group	Assigns a name to a list of User objects in the Directory. You can assign rights to the group instead of to each user—the rights transfer to each user in the group. (See “Group object.”)
License Certificate	Used with NetWare Licensing Services (NLS) technology to install product license certificates as objects in the Novell Directory database. License Certificate objects are added to the Licensed Product container when an NLSaware application is installed.
LSP Server	A leaf object that represents a NetWare® server with the NetWare Licensing Services NLM loaded.
Message Routing Group	Represents a group of messaging servers that can transfer messages directly among themselves. (See “Message Routing Group object.”)
Messaging Server	Represents a NetWare MHS server that resides on a NetWare server. A NetWare MHS Server object is automatically created in the Directory tree when you install NetWare MHS on a NetWare server. (See “Messaging Server object.”)

Leaf object	Description
NetWare Server	Represents a server running any version of NetWare. (See “NetWare Server object.”)
Organizational Role	Defines a position or role within an organization. (See “Organizational Role object.”)
Print Queue	Represents a network print queue.
Print Server	Represents a network print server.
Printer	Represents a network printing device.
Profile	Represents a login script used by a group of users who need to share common login script commands but who aren't necessarily located under the same container in the Directory tree, or who are a subset of users in the same container.
User	Represents the people who use your network. (See “User object.”)
Unknown	Represents an NDS object that has been corrupted and can't be identified as belonging to any of the other object classes.
Volume	Represents a physical volume on the network. (See “Volume object.”)

Location of Objects in the Directory Tree

In a Directory tree, you can place container objects and leaf objects in different configurations, according to your company’s needs. The following figure shows possible configurations:

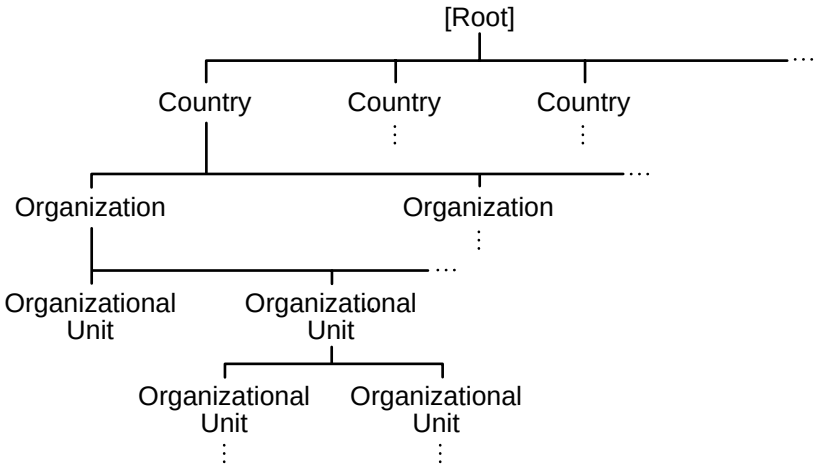
Figure 14-2
Possible Configurations for a Directory Tree



The Country and Organizational Unit objects are optional, but you must include at least one Organization object in your Directory tree.

You aren't limited to using only one container object in a tree; you can use many at each level. The following figure shows an example Directory tree that has several container objects at each level:

Figure 14-3
Example Directory Tree with Several Container Objects



Object Names

The path from an object to the root of the Directory tree forms the object's *complete name* , which is a unique name. Most leaf objects also have a *common name* . For User objects, the common name is their login name, displayed in the Directory tree.

Other leaf objects also have common names displayed in the Directory tree, such as a Printer object name or a Server object name.

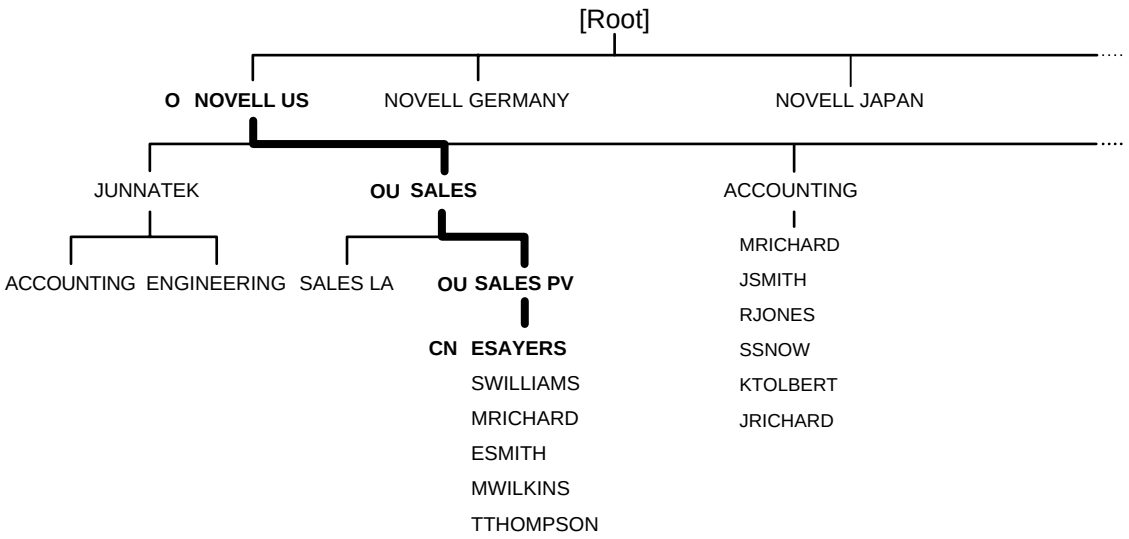
Container objects don't have common names. They are referred to by their Organizational Unit name, or Organization name, or Country name.

An object's complete name consists of its common name (if it has one), followed by a period (.), then the name of the container object, also followed by a period, and on up through succeeding container object names to the root of the tree.

For example, in the following figure the complete name for ESAYERS would be

ESAYERS.SALES PV.SALES.NOVELL US

Figure 14-4
Complete and Common Names



When querying the Directory, you can supply the object's complete name to receive information that describes that object.

Or, you can supply an object's property value and receive a list of object names that have that value.

For example, to find all users with a last name of Smith, search for Smith in the last name property of User objects.

Object Contexts

NDS allows you to refer to objects according to their positions within a tree. When you add an object (such as a server or user) to the network, you place that object in a container object in the Directory tree.

The position of the object within its container is its *context* . For example, in the previous figure, the context for User object ESAYERS is SALES PV.SALES.NOVELL US.

When you move from one container object to another, you *change contexts* . Whenever you change contexts, you must indicate the complete name of the object you are changing contexts to. (If you're changing to a context that

includes spaces between words, be sure to include an underscore in place of the space.)

If you are referring to an object in the same container object as your User object, then you need only refer to that object by its common name, not its complete name.

For example, in the previous figure, if ESAYERS located in SALES PV.SALES.NOVELL US wants information on ESMITH located in the same context, then ESAYERS need only refer to the User object as ESMITH.

Object Properties

Each type of object has certain properties that hold information about the object.

For example, some User object properties include the login name, password restrictions, and group memberships. Some Profile object properties are the profile name, login script, and volume.

The only properties *required* for objects are those you enter when you create a new object. You must enter a value in each field.

Properties you must specify when you create an object are

- Properties that name the object
- Properties required to create the object but that don't name it

  For example, when you create a Volume object, you must specify the volume's host server.

Many of an object's properties can contain multiple values. For example, the telephone number property, found in many object types, can contain several different telephone numbers.

The NETADMIN and NetWare Administrator utilities allow you to see and change properties for any object to which you have sufficient rights.

See also “Novell Directory Services” ; Object Rights in *Supervising the Network* .

Object rights

Qualities assigned to an object that control what the object can do with directories, files, or other objects.

See “Rights.”

ODI

(Open Data-Link Interface) An architecture that allows multiple LAN drivers and protocols to coexist on network systems.

See “Open Data-Link Interface.”

ODINSUP

(Open Data-Link Interface Network Driver Interface Specification Support) An interface that allows the coexistence of two network driver interfaces: Network Driver Interface Specification (NDIS) and ODI. (See also “Open Data-Link Interface.”)

ODINSUP allows you to connect to dissimilar networks from your workstation and use them as if they were one network.

ODINSUP also allows NDIS protocol stacks to communicate through the ODI's LSL and MLID. This way, NDIS and ODI protocol stacks can coexist in the same system, making use of a single ODI MLID.

For example, after you load ODINSUP on your workstation, you can log in to 3Com* 3+Share*, Microsoft LAN Manager, or IBM LAN Server network, and also log in to a NetWare network, using the same network board in the workstation.

You can then copy files and run applications between the two networks as if they were one.

When ODINSUP is loaded, you can use a wider variety of programs without having to worry about compatibility and without reconfiguring or rebooting your workstation to switch from one type of network to another.

ODINSUP functions as a default protocol stack. As a default protocol stack, it accepts packets from the ODI Link Support Layer (LSL) that aren't specifically marked with a protocol identifier (PID) for registered ODI protocol stacks (such as IPX or TCP/IP).

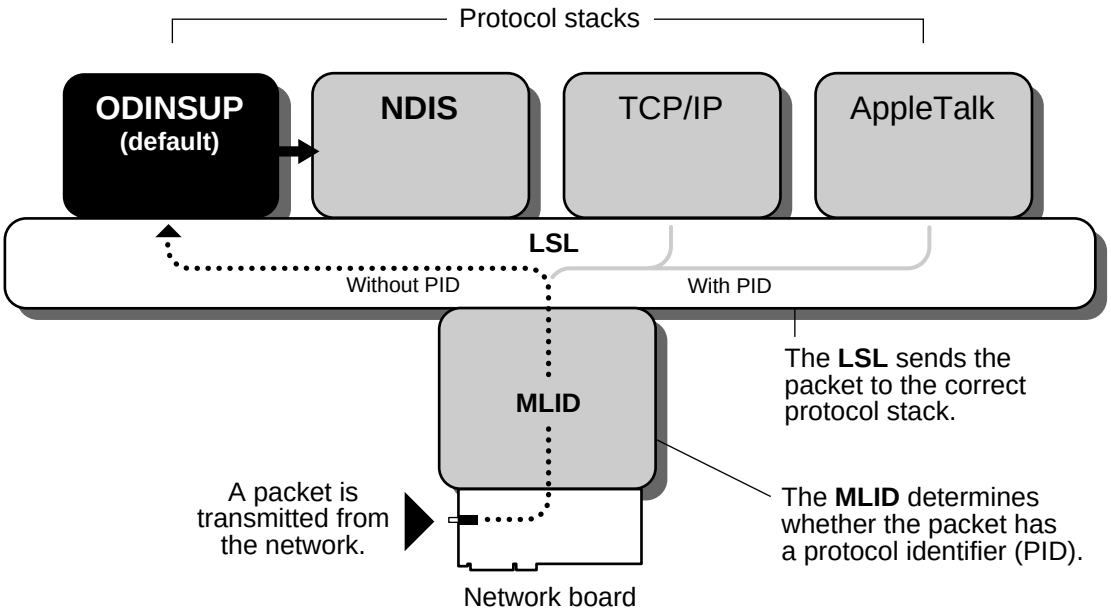
When it receives a packet, ODINSUP provides the packet to the NDIS Protocol Manager and passes it on to the NDIS protocol stack.

ODINSUP allows the NDIS protocol stack to communicate with a network board.

The NDIS protocol stack acts as though it is communicating with the network through an NDIS 2.0 MAC driver, and isn't aware of the ODINSUP protocol stack.

The details of the packet's transmission are handled by the MLID, which is the ODI driver. This is illustrated in the following figure:

Figure 14-5
ODINSUP



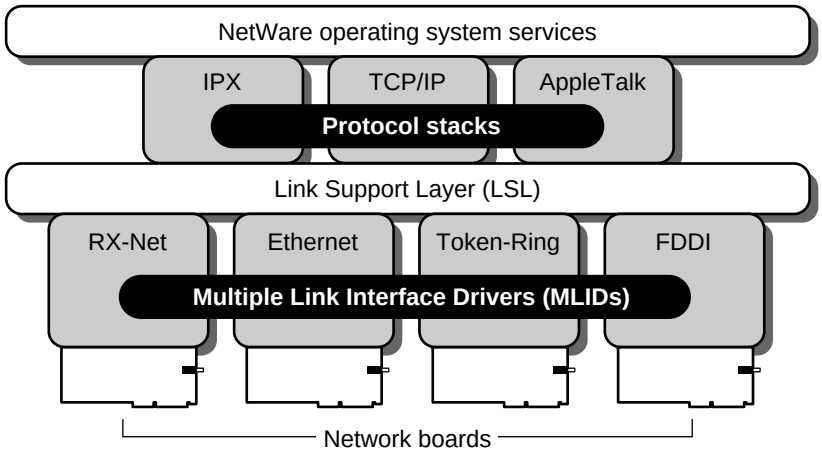
Open Data-Link Interface

(ODI) An architecture that allows multiple LAN drivers and protocols to coexist on network systems.

ODI describes the set of interface and software modules used to decouple device drivers from protocol stacks and to enable multiple protocol stacks to share the network hardware and media transparently.

The following figure illustrates the components of the ODI model in the server environment:

Figure 14-6
ODI Model



The major components of the ODI architecture are described in the following sections.

Multiple Link Interface Driver (MLID)

The MLID is a device driver written to the ODI specification that handles the sending and receiving of packets to and from a physical or logical LAN medium.

Each driver is unique due to the adapter hardware and media, but the ODI eliminates the need to write separate drivers for each protocol stack.

ODI allows LAN drivers to function with protocol stacks independently of the media frame type and protocol stack details.

An MLID interfaces with a network board and handles media frame header appending and stripping.

They also help demultiplex the incoming packets by determining their frame format.

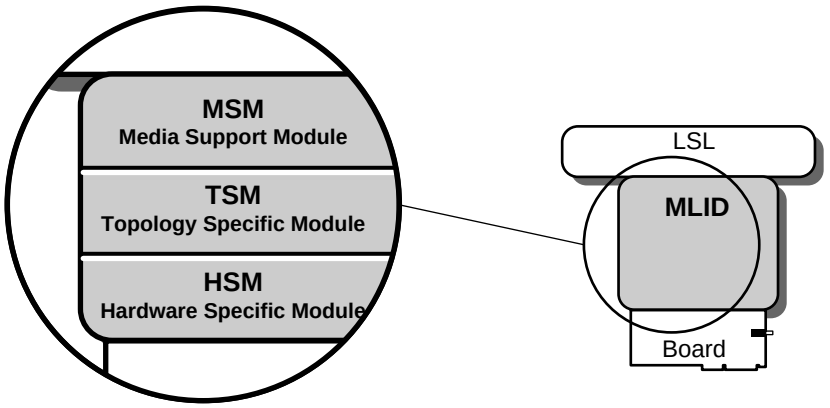
Novell has made ODI LAN driver development easier by furnishing a set of support modules that provide all tools necessary to interface a LAN driver to the LSL.

These modules are the Media Support ModuleTM (MSM), which contains general functions common to all drivers, and the Topology Specific ModuleTM (TSM), which provides support for the standardized media types of Ethernet, token ring, RX-Net, and FDDI.

These modules and the Hardware Specific ModuleTM (HSM) are described later in this section.

The following figure illustrates the modules which make up an MLID. Note that in the server environment, the MSMTM, TSMTM, and HSMTM are modules that are loaded separately.

Figure 14-7
MLID Modules



In the DOS environment, the MSM and TSM are linked in with the HSM so that only one module is loaded.

Link Support Layer (LSL)

The LSL is a software module that interfaces between drivers and protocol stacks. It essentially acts like a switchboard, directing packets between the drivers and protocol stacks.

Any ODI LAN driver can communicate with any ODI protocol stack through the LSL. The LSL handles the communication between protocol stacks and MLID software.

Because the ODI allows the physical LAN medium to support many different types of protocols (for example, IPX, TCP/IP, AppleTalk, and LAT might all

be supported on one Ethernet network adapter), the MLID receives packets destined for different protocol stacks that might be present in the system.

The LSL then determines which protocol stack the packet should be delivered to. Next, the protocol stack determines what should be done with the packet.

When the protocol stack must transmit a packet, the protocol stack returns the packet to the LSL, which then routes the packet to the appropriate MLID.

The LSL enables the protocol stacks to handle sending and receiving.

The LSL also tracks the various protocols and MLID software loaded in the system. It also provides a consistent method of finding and using each of the loaded modules.

Media Support Module (MSM)

The MSM standardizes and manages primary details of interfacing ODI MLID software to the LSL and operating system.

The MSM handles generic initialization and runtime issues common to all drivers.

Topology Specific Module (TSM)

The TSM manages operations unique to a specific media type, such as Ethernet or token ring. Multiple frame support is implemented in the TSM so that all frame types for a given media are supported.

Hardware Specific Module (HSM)

The HSM is created for a specific network board. The HSM handles all hardware interactions. Its primary functions include adapter initialization, reset, shutdown, and removal.

It also handles packet reception and transmission. Additional procedures may also provide support for timeout detection, multicast addressing, and promiscuous mode reception.

Open Shortest Path First

(OSPF) A link state internal gateway protocol. OSPF is part of the TCP/IP protocol suite.

Link state routers exchange information about the state of their network connections or links. Using this information, each router can construct the topology of the internetwork and derive routing information.

This method is generally considered superior when compared to using distance vector routing protocols, which have little direct knowledge of the network's topology.

OSPF routers exchange information using link state advertisements. For each destination, the router examines its link state database and selects the shortest path as the route to that destination.

The link state information is then shared with other routers to varying degrees as determined by how the routers in your network are grouped and how they are related to each other.

For administrative purposes, the OSPF internetwork can be divided into different regions, called areas. All routers within an area share complete link state information.

The route information shared between areas can be filtered and is generally a distillation of the rest of the autonomous system's topology.

Optical disc

(Also *optical disk*) A form of removable media used to store data. An optical disc can be one- or two-sided. Some optical discs are read-only; others can be read from and written to.

HCSS uses rewritable optical discs.

See also "High Capacity Storage System."

Optical disc library

A high-capacity storage device, sometimes called a *jukebox* , that uses an autochanger mechanism to mount and dismount optical discs as needed.

See also “High Capacity Storage System.”

Organization object

A container object that helps you organize other objects in the Directory and allows you to set template information for users created in it.

For example, you could use an Organization object to represent a company, or a university with various departments, or a department with several project teams.

The Organization object is a level below the Country object (if used), and a level above the Organizational Unit object (if used).

See also “Object” ; Creating Container Objects in *Supervising the Network* .

Organizational Role object

A leaf object that defines a position or role within an organization. Use the Organizational Role object to specify a position that can be filled by different people, such as Team Leader or Vice President.

See also “Object” ; Managing Organizational Role Objects in *Supervising the Network* .

Organizational Unit object

A container object, a level below the Organization object, that helps you to further organize objects in the Directory and also allows you to set template information for users created in it.

For example, an organizational unit could be a division, a business unit, a project team, or a university department within your organization. You can use an Organizational Unit object to logically arrange these entities in your directory tree.

See also “Object” ; Creating Container Objects in *Supervising the Network* .

OSPF

(Open Shortest Path First) A link state internal gateway protocol. OSPF is part of the TCP/IP protocol suite.

See “Open Shortest Path First.”

Owner

The user who creates a file or directory. A file or directory owner does not inherit special access rights in NetWare.

If the administrator has set per-user disk space restrictions, then the file owner is used to identify the user who is charged for the disk space associated with a file or directory.See also “Disk space restrictions” ; “Rights.”

Chapter 15 *P*

Packet

A unit of information used in network communication.

Messages sent between network devices (such as workstations or NetWare servers) are formed into packets at the source device.

The packets are reassembled, if necessary, into complete messages when they reach their destination.

A packet might contain a request for service, information on how to handle the request, and the data to be serviced.

An individual 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 packet arrives at its destination, the headers are stripped off in reverse order and the request is serviced.

For example, 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 MLID adds a hardware or MAC frame header.

See also "Communication protocols" ; "Ethernet configuration" ; "Large Internet Packet" ; "NetWare Core Protocol."

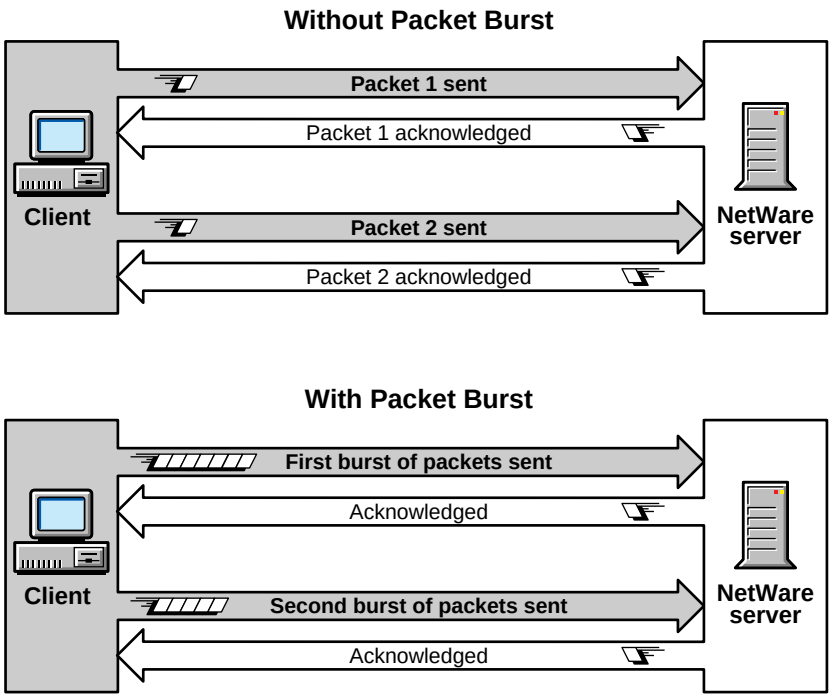
Packet Burst protocol

A protocol built on top of IPX that speeds the transfer of multiple-packet NCP file reads and writes.

The Packet BurstTM protocol speeds the transfer of NCP data between a workstation and a NetWare server by eliminating the need to sequence and acknowledge each packet.

Packet Burst protocol is more efficient than the one-request/one-response protocol in earlier NetWare versions. With Packet Burst protocol, the server or workstation can send a whole set (burst) of packets before it requires an acknowledgment.

Figure 15-1
Packet Burst Protocol



By allowing multiple packets to be acknowledged, Packet Burst protocol reduces network traffic.

Packet Burst protocol also monitors dropped packets and retransmits only the missing packets.

NetWare 4 doesn't require an NLM to enable Packet Burst at the server. For workstations to send and receive Packet Burst data, you must enable Packet Burst under the NetWare DOS Requester.

When Packet Burst-enabled servers or workstations transfer data to servers or workstations that don't have Packet Burst enabled, the data defaults to normal NCP mode (one-request/one-response).

Packet receive buffer

An area in the NetWare server's memory set aside to temporarily hold data packets arriving from the various workstations.

The packets remain in this buffer until the server is ready to process them and send them to their destination. This ensures the smooth flow of data into the server, even during times of particularly heavy input/output operations.

The number of packet receive buffers is set during server installation. This number is increased by the operating system as needed due to heavy buffer activity, within the following parameters (also set during server installation).

- **Maximum packet receive buffers** The *maximum* number of packet receive buffers that the operating system can allocate.

- **Minimum packet receive buffers** The *minimum* number of packet receive buffers that the operating system can use.

- **New packet receive buffer wait time** The operating system can increase the number of packet receive buffers as needed, within the set parameters.

  However, rather than allocating a new packet immediately on demand, the operating system waits for the specified time, after which the packet is allocated if still needed.

  This ensures that new packet receive buffers aren't allocated needlessly due to sporadic peak activity.

  If the set maximum number of packet receive buffers is reached, and a waiting packet isn't processed within the specified wait time, the operating system discards the packet, and the station must resend the packet.

The default range of packet receive buffers should be satisfactory for most server installations, even with many users performing many read/write operations.

Because more system overhead is required to manage large numbers of packet receive buffers, we recommend that you increase the maximum range *only* if you are running out of buffers.

For example, if your server is slow when first brought up, but later speeds up, the minimum packet receive buffer setting may be too low. The delay is caused by the accumulation of packet receive buffer wait times. If your server always allocates at least 200 packet receive buffers, set the minimum to 200.

See also “Watchdog.”

Paging

Allows NetWare 4 to assign memory noncontiguously. This is a feature of most high-powered CPU architectures (such as the Intel* 80386/80486 and the Pentium*).

Rather than assign memory to processes in large blocks of contiguously-addressed pages, NetWare 4 uses segmentation to assign memory noncontiguously.

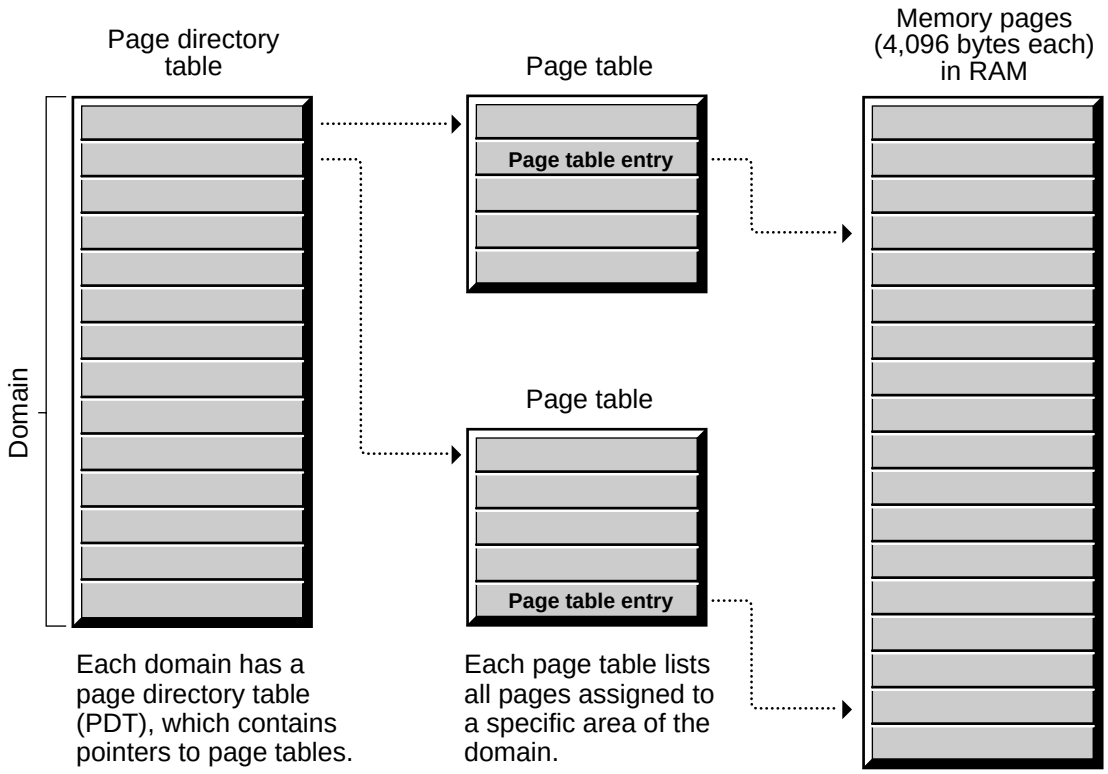
Page tables are used to map physical addresses to logical memory. Each page table entry corresponds to a page in memory. A memory page is a 4KB block of RAM. A group of page tables is a *domain* .

Other systems sometimes use paging to create virtually contiguous blocks from physically non-contiguous blocks of memory. The NetWare operating system doesn't use paging for this purpose.

The main function of paging in NetWare is for memory protection. For instance, NetWare maps out certain memory addresses to prevent access to those pages in memory.

A domain's page tables are listed in the page directory table.The two levels of lookup tables in NetWare 4 are illustrated in the following figure:

Figure 15-2
Paging



Parallel port

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

See also “LPT ports” ; Selecting the Best Type of Printer for Your Setup in *Print Services* .

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 “File system.”

Parent objects

Container objects that contain other objects.

See “Object.”

Parity

A method of checking for errors in transmitted data.

See “Serial communication.”

Partition (disk)

A logical unit into which NetWare server hard disks can be divided.

See “Disk partition.”

Partition (Novell Directory)

A logical division of the Novell Directory database.

See “Novell Directory partition.”

Partition management

The method of managing Novell Directory partitions and replicas.

Partition management allows you to divide the Directory into partitions and manage various Directory replicas of these Directory partitions.

Partition management allows you to

- Create, merge, and move Directory partitions
- Display partitions and partition details

- Add, delete, synchronize, and display Directory replicas

Related utilities: NetWare Administrator and NDS Manager in *Utilities Reference* .

Passive hub

A device used in some network topologies to split a transmission signal, allowing additional workstations to be added.

See “Hub.”

Password

The characters a user must type to log in. NetWare allows the network supervisor to specify whether passwords are required and, if so, to assign a login password to each user on the network.

The network supervisor can also specify whether passwords must be unique and whether they must be changed periodically.

In NetWare 4, login passwords are encrypted at the workstation and put into a format that only the NetWare server can decode. This format helps prevent intruders from accessing network files.

See also “Security” ; “User object.”

Path

The location of a file or directory in the file system.

For example, the path for file REPORT.FIL in subdirectory ACCTG in directory CORP on volume SYS: of server ADMIN is

ADMIN\SYS:CORP\ACCTG\REPORT.FIL

See also “Authentication” ; “File system.”

Physical memory

The RAM installed in a computer.

NetWare servers use paging to address physical memory in 4KB blocks, or pages.

See also “Logical memory” ; “Paging.”

Polled mode

A printer configuration option through which the port driver (NPRINTER) periodically checks, or polls, the data port to determine whether it is ready to accept data for transmission to the printer.

The port's status is indicated by an electronic signal called a flag. Polling queries are made at each CPU timer tick (18 times per second).

In NetWare 4, polled mode is the default for printer configurations. Using polled mode allows users to set up a printer without having to determine which interrupt the port is set to or whether the port supports interrupts.

In earlier releases of NetWare, polled mode with RPRINTER was considerably slower than the alternative interrupt mode.

However, the enhanced performance of NPRINTER for NetWare 4 makes polled mode considerably faster than before. In most instances, users see little difference in performance between polled mode and interrupt mode.

The advantage of polled mode is that it eliminates any possibility of interrupt conflicts among different hardware configurations. (However, I/O port addresses must still be unique.)

In complex printing setups with multiple printers running off a single workstation, polled mode may noticeably slow other tasks on that workstation.

Port (hardware)

A connecting component that allows a microprocessor to communicate with a compatible peripheral, such as a printer.

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.

Port driver

A driver that routes print jobs out of the and through the proper port (for example, LPT1, LPT2, COM1) to the printer that will handle the job. The NPRINTER utility functions as a port driver in NetWare.

Postmaster

A user who has all of the following rights:

- Supervisor access to the NetWare MHS Messaging Server object
- Supervisor access to the Mailbox Location, Mailbox ID, and E-mail Address properties of users of the NetWare MHS messaging server
- Read access to the Message Routing Group that the NetWare MHS messaging server is in

Basic NetWare MHS sends a message to the Postmaster's mailbox when certain types of errors occur. For example, if a message is not in valid NetWare MHS format, the NetWare MHS Messaging Server cannot determine who the sender is. So, it sends a message to the Postmaster.

Postmaster General

A user who has Supervisor access to the Message Routing Group that he or she resides in. A Postmaster General can add a messaging server to, or remove a messaging server from, the Message Routing Group.

You can assign several Postmasters General to a Message Routing Group.

Primary server

The SFT III NetWare server that has been operating longer than its partner and is currently servicing workstations.

The primary server is the SFT III server that network workstations see, and the one to which they send requests for network services. Routers on the internetwork see only the primary server and send routing packets to it.

The primary server's IOEngine determines the order and type of events that are sent to the MSEngine. Only the primary server sends reply packets to network workstations.

The secondary server is the SFT III NetWare server that is activated after the primary server. Either server may function as primary or secondary, depending on the state of the system.

You cannot permanently designate which server is primary or secondary; system failure determines each server's role. When the primary server fails, the secondary server becomes the new primary server.

When the failed server is restored, it becomes the new secondary server.

Primary time server

A server that synchronizes the time with at least one other Primary or Reference time server, and provides the time to Secondary time servers and to workstations.

See "Time synchronization."

Print device definition

A set of functions and modes found in a file with a .PDF extension that corresponds to a printer, plotter, or other peripheral.

A print device definition does not necessarily represent the full functionality of the printer. A print device definition can be modified to change the functions the machine can perform.

Print device definitions contain the necessary control sequences for setting or resetting the printer and for controlling bold, emphasis, italics, print size, font selection, colors, and other features, depending on the printer.

If your application does not have the print driver for your printer, NetWare supplies the control sequences in the form of print device definitions for many common printers.

These print device definitions are copied to the SYS:PUBLIC directory during installation. Each print device definition has a .PDF (print device function) extension.

Definitions required for your environment must be imported into NetWare print services using the NetWare Administrator or PRINTDEF.

If your printer does not match the predefined print devices, you can create a print device by defining the correct control sequences in the NetWare Administrator or PRINTDEF. The control sequences for your machine are found in your printer manual.

Print device definitions also allow you to specify modes (groups of one or more functions) for use in print job configurations. Modes can prepare the printer for a print job, combine functions, reset the printer back to default settings, etc.

You specify print device modes using the NetWare Administrator or PRINTDEF. These modes can then be included in print job configurations you create in PRINTCON. The NPRINT, CAPTURE, and PCONSOLE utilities use the print job configurations to send print jobs to your printer with the correct control sequences.

See also “Print header and print tail” ; Working with Print Device Definitions and Printer Forms in *Print Services* .

Print driver

A driver that converts print jobs (usually generated by an application) to a format that can be read by the type of printer being used.

Print header and print tail

Contain transport control codes for the modes defined in PRINTDEF.

The print header precedes the data to the print queue, and the print tail follows it. The default lengths are 64 and 16 bytes, respectively. These are especially critical for PostScript printing.

Print job

A file stored in a print queue directory waiting to be printed. As soon as a print server sends a print job to the printer, the print job is deleted from the queue directory.

Each print job is assigned a filename with a variation of the first four characters of the print queue directory ID, four more numerals, and a .Q extension.

For example, if the print queue directory is named 4B020057.QDR, the first print job to enter the empty print queue would be named 024B0001.Q.

If more print jobs entered the print queue before the current print job was printed, they would be named 024B0002.Q, 024B0003.Q, 024B0004.Q, etc.

As soon as print job 024B0001.Q is printed, the next print job to enter the print queue is named 024B0001.Q. Like all print jobs, it would follow the first-in, first-out basis, unless the print job was held, or a print queue operator changed the order of service.

Print jobs can be submitted to the print queue through NDS or through bindery services.

Print job configuration

A set of options that determine how a job is printed. The characteristics may include the following:

- Printer to be used
- Print queue to be used
- Number of copies to print
- Use of a banner page
- Printer form

- Print device mode

Users can create print job configurations using the NetWare Administrator or PRINTCON.

See also Printing Tasks Handled Through NetWare Administrator and Working with Print Device Definitions and Printer Forms in *Print Services* .

Print queue

A network directory that stores print jobs. When the printer assigned to a print queue is ready, the print server takes the print job out of the print queue and sends it to the printer.

The print queue can hold as many print jobs as disk space allows.

Print Queue Setup

When you create a print queue in NetWare Administrator or PCONSOLE, a corresponding directory is created.

In NDS, the print queue directory resides in the QUEUES directory on the volume specified.

In a bindery server, the print queue directory resides in the SYSTEM directory on volume SYS: of the current server.

The Quick Setup option in PCONSOLE automatically creates a print queue for each printer. This simplifies your printing setup. (See Planning and Setting Up NetWare Print Services in *Print Services* .)

When you create a print queue, user ADMIN is assigned as a print queue operator, and all users in the same context are assigned as print queue users.

To change these default assignments, use NetWare Administrator or PCONSOLE.

Group EVERYONE (if it exists) is also automatically assigned as a print queue user. (See also “Print queue operator.”)

Print Queue Directories and Filenames

The print queue directory is assigned a random number. This number is the print queue ID seen in NetWare Administrator with a .QDR extension. The number is also displayed in PCONSOLE without the extension.

If you name the queue according to the type or location of the printer, it is easier to remember which queue is serviced by which printer.

For example, print queue LETTERHEAD_Q might be directory LEGAL/SYS:QUEUES/4B020057.QDR if configured on NetWare server LEGAL. The print queue ID would then be 4B020057.

All print queue directories have the extension .QDR and contain files with .SYS and .SRV extensions that are flagged *hidden* and *system* . These files are visible with the NDIR utility.

These filenames begin with Q_ and use a variation of the first four digits of the print queue directory ID.

The print queue directory in the previous example would contain hidden and system files named Q_024B.SYS and Q_024B.SRV. (See also “Print job.”)

See Managing Print Services with the NetWare Administrator Utility and Managing Print Services Using PCONSOLE in *Print Services* .

Print queue operator

A user who can edit other users' print jobs, delete print jobs from the print queue, or modify the print queue status by changing the operator flags.

Print queue operators can also change the order in which print jobs are serviced.

User ADMIN or equivalent can assign users to be print queue operators as necessary.

See also Managing Print Services with the NetWare Administrator Utility and Managing Print Services Using PCONSOLE in *Print Services* .

Print server

A server that takes print jobs out of a print queue and sends them to a network printer.

NetWare print servers run through PSERVER.NLM on a NetWare 4 server and can service up to 255 printers with any number of print queues assigned to the printers.

In NetWare 3, print servers are loaded through either PSERVER.NLM on a file server or PSERVER.EXE on a dedicated workstation.

See also Setting Up and Servicing Print Servers in *Print Services* .

Print Server object

A leaf object appearing in the Directory tree that represents a network print server.

See also “Object” ; “Print server” ; Setting Up and Servicing Print Servers in *Print Services* .

Print Server operator

A user or member of a group delegated rights by User object ADMIN to manage the print server.

A print server operator has rights to control notify lists, printers, and queue assignments.

See also Managing Print Services with the NetWare Administrator Utility and Managing Print Services Using PCONSOLE in *Print Services* .

Print Server Status and Control Protocol

(PSSCP) An SPX-based communications protocol that requests certain services from the print server (PSERVER.NLM).

Network users and administrators can perform services such as requesting the status of print jobs, deleting print jobs, or changing forms. A user can only access his or her own job; an operator can access any print job.

Print tail

Contains transport control codes for the modes defined in PRINTDEF.

See “Print header and print tail.”

Printer

A peripheral piece of hardware used to produce printed material.

Network printers can be attached

- Directly to the network
- To the printer port of a NetWare server
- To the printer port of a PC workstation

In NetWare 4, users can specify printer names as the destination of their print jobs. (Users can still specify print queues.)

In NetWare 3, users must specify the print queue.

Network Printer Drivers

Every network printer requires a network printer port driver to pass a print job from the network to the printer. The type of driver depends on how the printer is attached to the network.

Network-attached printers store their own port drivers.

Printers attached to workstations need NPRINTER.EXE loaded on the workstation.

Printers attached to NetWare servers need NPRINTER.NLM loaded on the NetWare server.

Note

If PSERVER.NLM is loaded on the same NetWare server, it can load NPRINTER.NLM automatically for each printer cabled directly to the NetWare server.

Differences between the Bindery and Novell Directory Services

In bindery-based NetWare, printers are defined as a subset of the print server. For that reason, a print server must exist before you can define a printer.

With NDS, printers are objects used in conjunction with Print Server and Print Queue objects. They can be added, modified, or removed independently.

Each network printer object must be defined using NetWare Administrator or PCONSOLE.

See also “Printing” ; “Print device definition” ; Setting Up and Servicing Printers in *Print Services* .

Printer Communications Protocol

(PCP) An SPX-based protocol used by printer drivers (NPRINTER.NLM and NPRINTER.EXE) to communicate with print servers (PSERVER.NLM).

Printer form

A print option designed to prevent print jobs from being printed on the wrong paper.

NetWare print services allows you to designate a printer form for a print job. The print jobs will not print if the correct paper is not in the printer.

For example, suppose your printer uses regular, letterhead, and bond paper. For each type of paper, you can create a printer form. Each form has a unique name and number (between 0 and 255).

If you specify a form in a print job configuration, in NPRINT, or in CAPTURE with the form option, the print job does not print unless the mounted form matches the number required by the print job.

You can change the number of the currently mounted form at the print server console, from NetWare Administrator, or from PCONSOLE.

Printer forms are defined using NetWare Administrator or PRINTDEF.

See also Managing Print Services with the NetWare Administrator Utility ; Managing Print Services Using PCONSOLE ; and Working with Print Device Definitions and Printer Forms in *Print Services* .

Printer mode

A sequence of print functions (also called *printer commands* , *control sequences* , or *escape sequences*) that determines the appearance of the printed file.

A printer mode can define the style, size, boldness, and orientation of the typeface.

Print device modes are designated using NetWare Administrator or PRINTDEF.

See also Managing Print Services with the NetWare Administrator Utility and Working with Print Device Definitions and Printer Forms in *Print Services* .

Printer object

A leaf object that represents a physical printing device on the network.

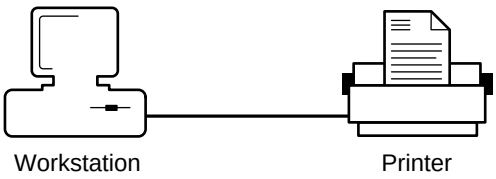
See also “Object.”

Printing

The ability to transfer data from computer files to paper.

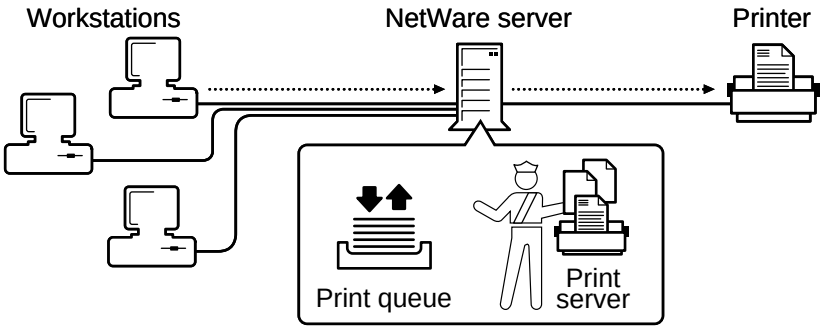
NetWare 4 allows users to share printers on the network, where previously each personal computer had to have a printer attached to one of its printer ports.

The following figure shows non-network printing:



NetWare 4 uses a print queue and print server to allow workstations to print to a printer. The print server takes print jobs from the print queue and sends them to the printer.

Figure 15-3
Network Printing



See also “Print server” ; “Print queue” ; “Printer” ; Introduction to NetWare Print Services in *Print Services* .

Profile login script

A type of login script that sets environments for a group of users. Use profile login scripts if there are groups of users with identical login script needs.

Profile login scripts are optional; if used, they execute after the container login script and before the user login script.

See also “Login scripts.”

Profile object

A leaf object that represents a login script used by a group of users who need to share common login script commands.

The group of users need not be located under the same container in the Directory tree. They can also be a subset of users in the same container.

See also “Object” ; Managing Profile Objects in *Supervising the Network* .

Prompt

A character or message 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, by default, displays the current drive letter followed by a > symbol (for example, F>)
- The NetWare server console prompt, which displays a colon (:)

The DOS prompt is a DOS environment setting. You can change the DOS prompt using the SET PROMPT command in a batch file (such as AUTOEXEC.BAT), in the login script, or at the command line.

For example, to change your DOS prompt at the command line so that the prompt displays the current drive mapping followed by the > symbol, you would type

SET PROMPT=PG <Enter>

See your DOS manual for further details on changing prompts, including prompt variables. (The NetWare server console prompt can't be changed.)

See also “Drive mapping” ; “Login scripts.”

Property

A characteristic of an NDS object. Each type of object (such as a User object, Organization object, or Profile object) has certain properties that hold information about the object.

For example, a User object's properties include login name, E-mail address, password restrictions, group memberships, etc.

As another example, a Profile object's properties include profile name, login script, and volume.

The only properties *required* for objects are those you enter when you create a new object. You must enter a value in each field.

Properties you must enter when you create an object can be properties that name the object, or properties required to create the object.

For example, when you create a volume object, you must specify the volume's host server.

Many of an object's properties can contain multiple values. For example, the telephone number property, found in many object types, can contain several different telephone numbers.

NETADMIN and NetWare Administrator allow you to see and change properties for any object to which you have sufficient rights.

See also "Object."

Property rights

Rights that apply to the properties of an NDS object.

See also "Rights."

Protocols

Conventions or rules used by a program or operating system to communicate between two or more endpoints.

See also "Communication protocols" ; "NetWare protocols and transports."

Proxy ARP

A technique by which a router replies to an Address Resolution Protocol (ARP) request from a host on behalf of the ARP target host.

Proxy ARP enables a router to support routing within a subnetted IP network with hosts that do not recognize the subnetting. In this situation, knowledge of the subnets is limited to the subnet routers, and the hosts see only the IP network.

By letting the subnet routers reply to ARP requests from hosts on behalf of hosts on other subnets reachable through the router, the hosts do not have to know about the subnets attached to the network. This use of Proxy ARP is referred to as *ARP subnet routers* .

However, because most IP hosts now understand subnetting, ARP subnet routers are not used as often as they once were. Instead, the network configuration, called *stub subnetworks* or *stub networks* , is now the most common use of Proxy ARP.

A stub network is a segment that has an address range that is a subset of the address range of another segment (the parent network).

The parent network and the stub network are separated by a router. An example is a parent network with an address range of 89.0.0.1 to 89.255.255.254 and a stub network with an address range of 89.1.0.1 to 89.1.255.254.

For more information on Proxy ARP, refer to RFC 1027.

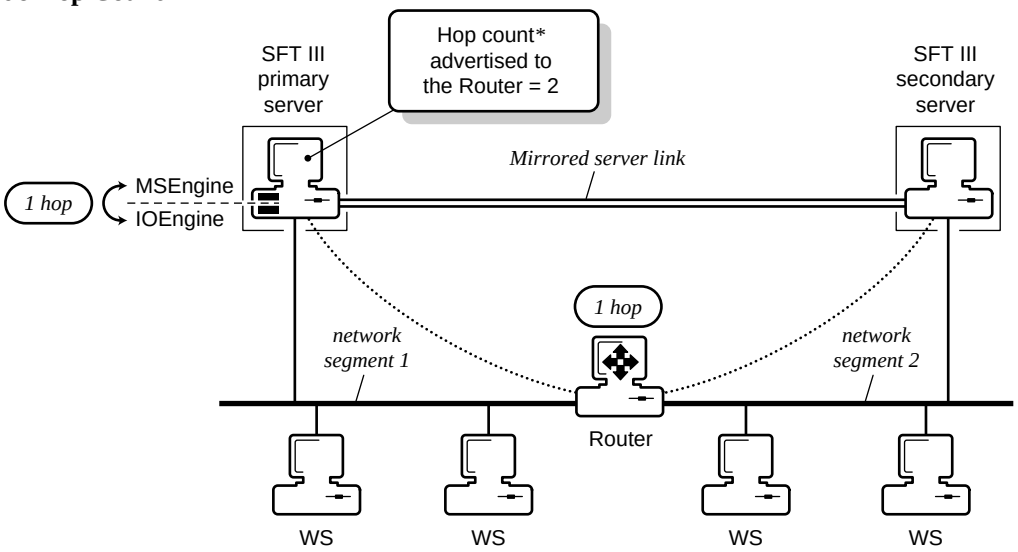
See also “Address Resolution Protocol.”

Pseudo hop count

The number of hops that the primary server adds to the true hop count (the number of internal and external bridges and routers between a client and the server) when it advertises the route to the SFT III MSEngine.

If SFT III servers reside on different network segments, the hop count for one server is higher than the other. To ensure that packets are rerouted properly to the surviving server in the event one server fails, the primary server advertises an artificially high hop count—the true hop count plus a pseudo hop count, as shown in the following figure:

Figure 15-4
Pseudo Hop Count



**True hop count advertised to the router = 1.*

SFT III uses the pseudo hop count to accelerate routing changes when a server switchover occurs in mirrored servers on different network segments.

Note

If the SFT III servers are installed on the same network segment, there are no routers and SFT III does not use the pseudo hop count.

If the primary server fails, the surviving server advertises the true hop count. Routers immediately see the surviving server as the best route to the MSEngine.

The total hop count (the true hop count plus the pseudo hop count) between a client and the server cannot exceed 16.

SET parameters enable the pseudo hop count and determine its maximum value.

PUBLIC directory

The SYS:PUBLIC directory, created during network installation, that allows general access to the network and contains NetWare utilities and programs for network users.

NetWare users running DOS have a search drive mapped to SYS:PUBLIC through the container login script and are assigned Read and File Scan rights to this directory.

Don't delete the PUBLIC directory.

See also "File system" ; "LOGIN directory" ; "MAIL directory" ; "SYSTEM directory."

Public files

Files that must be accessed by all NetWare users, including NetWare utilities, help files, and some message and data files.

By convention, the files are located in SYS:PUBLIC for DOS users.

All NetWare users have Read and File Scan rights to the files.

Public trustee

A special trustee that can be added to any object, directory, or file. By default, [Public] includes the Read right and the File Scan right.

By making [Public] a trustee of an object, directory, or file, you effectively grant all objects in NDS rights to that object, directory, or file.

[Public] is only used in trustee assignments and must always be entered within square brackets. [Public] can be added or deleted like any other trustee. An Inherited Rights Filter blocks inherited rights for [Public] as it would any other trustee.

Assigning [Public] as a trustee is similar to granting trustee rights to user GUEST or group EVERYONE in previous NetWare versions.

You can make [Public] a trustee of areas that every object should have access to. (A user doesn't have to log in to access areas where [Public] is granted rights.)

However, in most cases, it is better to make a container object a trustee rather than making [Public] a trustee. This grants rights only to the objects within the container, improving security control.

During installation, [Public] is granted the Browse object right at the root object of the Directory tree.

See also "Inherited Rights Filter" ; "Trustee."

Purge (P) attribute

A file system attribute that causes NetWare to purge the directory or file when it is deleted.

See also "Attributes."

Chapter 16 *Q*

Queue

A network directory that stores each print job. When the printer assigned to the print queue is ready, the print server takes the print job out of the print queue and sends it to the printer.

See “Print queue.”

See also Managing Print Services with the NetWare Administrator Utility and Managing Print Services Using PCONSOLE in *Print Services*.

Queue sampling interval

The time interval the print server waits between checking the print queues for jobs ready and waiting to be printed.

Queue server mode

An operating mode used by many network-direct printers and hardware queue servers produced by various manufacturers. These devices either connect to a printer and then to the network or are installed in a port at the printer.

In many cases, these devices offer a fast, effective, low-cost printing solution in NetWare 4 as well as NetWare 3 environments.

In queue server mode, the hardware print server directly accesses the print queue using NCP calls. Under most circumstances, this mode places the least load on a NetWare server. In NetWare 3, it was also faster than remote printer mode, but the improved performance of the NetWare 4 PSERVER has minimized this distinction.

Queues created in the bindery context can be seen by both NDS and bindery users, so both types of users can access these hardware print servers.

See also Using Third-Party Network-Direct Print Devices with NetWare 4 in *Print Services*.

Chapter 17 *R*

RAM

(Random Access Memory) The internal dynamic storage of a computer that can be addressed by the computer's operating system.

See also "Memory."

RARP

(Reverse Address Resolution Protocol) The process of determining the Internet address from a local data link address.

See "Reverse Address Resolution Protocol."

Read-after-write verification

A means of assuring that data written to the hard disk matches the original data still in memory.

If the data from the disk matches the data in memory, the data in memory is released.

If the data doesn't match, the block location is recognized as bad, and Hot Fix redirects the data to a good block location within the Hot Fix Redirection Area.

See also "Data protection."

Read-only replica

The Directory replica used to view, but not modify, Directory information.

See “Novell Directory replica.”

Read Only (Ro) attribute

A file system attribute that indicates that no one can write to the file.

See also “Attributes.”

Read right

A file system right that grants the right to open and read files.

Also, a property right that grants the right to read the values of the property.

See also “Rights.”

Read/write replica

The Directory replica used to read or update Directory information (such as adding or deleting objects).

See “Novell Directory replica.”

Real mode

The mode that allows an 80286, 80386, or 80486 processor to emulate an 8086 processor and run as though it were an 8086 processor.

The 8086 processor uses a 20-bit address bus, and can address up to 1 MB of memory. The 8086 processor is also limited to running only one application or process at a time.

When running in protected mode, the 80286, 80386, and 80486 processors are capable of multitasking and addressing much more than 1 MB of memory.

When running in real mode, these processors are subject to the same 1MB memory constraint as the 8086 processor, and they can run only one application or process at a time.

However, the 80286, 80386, and 80486 processors running in real mode still perform more efficiently than the 8086 processor because they operate at a faster clock rate.

Record locking

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

Redirection area

(Hot Fix Redirection Area) The space on a hard disk set aside to hold data redirected from faulty disk blocks.

See “Hot Fix.”

Reference time server

A server that specifies the time to which all other time servers and workstations synchronize.

See also “Time synchronization.”

Remote boot

A method that allows a user to boot a workstation from remote boot image files on a NetWare server rather than from a boot diskette in the workstation's local drive.

Client workstations that can start using remote booting do not need a floppy or hard drive to function on the network, and are therefore called *diskless workstations* .

A diskless workstation relies on a Programmable Read Only Memory (PROM) chip installed in its network board to communicate with the boot server.

NetWare allows you to use a default image file for all diskless workstations on the network or to use customized image files unique to each workstation's particular system and network environment.

See also "Remote printer mode."

Remote connection

A connection between a LAN on one end and a workstation or network on the other, often using telephone lines and modems.

A remote connection allows data to be sent and received across greater distances than those allowed by normal cabling.

Remote console

Software that allows network supervisors to manage servers from a workstation.

To create a remote console session, invoke the RCONSOLE.EXE client utility.

RCONSOLE enhances security since you can lock servers in a safe place and remove the keyboards and monitors.

From a remote console, network supervisors can

- Use console commands as if they were at the server console
- Scan directories and edit text files in both NetWare and non–NetWare partitions on a server
- Transfer files to (but not from) a server
- Bring down a server
- Install or upgrade NetWare on a remote server

You can set up *direct* or *asynchronous* connections to a server:

- **Direct connection.** A station establishes a remote console session with a server on the local or wide area network, connected by cabling or by a wide-area link using IPX/SPX protocol.

- **Asynchronous connection.** A station establishes a remote console session with a server through a modem or null modem cable.

See also Using Remote Console to Manage a Server in Chapter 7 of *Supervising the Network* .

Remote printer mode

An operating mode used by many network-direct printers and hardware queue servers produced by various manufacturers.

Network-direct printers and hardware queue servers either connect to a printer and then to the network or are installed in a port at the printer. In many cases, these devices offer a fast, effective, low-cost printing solution in NetWare 4 and NetWare 3 environments.

In this mode, the device functions in a way similar to a workstation running NetWare 4 NPRINTER or NetWare 3 RPRINTER. Devices configured for remote printer mode are controlled by a NetWare print server.

Devices running in this mode under NetWare 4 run considerably faster than they did under NetWare 3. The increased speed and flexibility offered with NetWare 4 makes remote printer mode a very effective way of providing network printing with these devices.

In order to run these devices in remote printer mode under NetWare 4, be sure you have loaded PSERVER.NLM at the NetWare server console.

See also Using Third-Party Network-Direct Print Devices with NetWare 4 in *Print Services* .

Remote Program Load

(RPL) Technology based on the concept of storing an image of a bootable floppy disk on a NetWare volume. Remote boot workstations use this image to start up the system prompt.

These client workstations do not need a floppy or hard drive to function on the network and are, therefore, called *diskless workstations* .

A diskless workstation relies on a programmable read-only memory (PROM) chip installed in its network board. This chip allows the workstation to communicate with the boot server.

When the workstation is turned on, it uses the boot image stored on a server to load the DOS system and Novell Client files necessary to connect to the network.

The image file can include any files you would normally load from a boot diskette.

NetWare allows you to use a default image file for all diskless workstations on the network, or to use customized image files unique to each workstation's particular system and network environment.

Remote Reset

Software that allows you to boot a DOS workstation (including a diskless workstation) from a remote boot image file on a NetWare server, rather than from a boot diskette in the workstation's local drive.

To use Remote Reset to boot a workstation, install a Remote Reset PROM on the station's network board and run the DOSGEN utility.

DOSGEN uploads the station's boot files into a remote boot image file, NET$DOS.SYS, in the server's LOGIN directory.

The remote boot image file includes the station's AUTOEXEC.BAT file, used by the station as if the file were present on a local boot diskette.

Copy the workstation's AUTOEXEC.BAT file to the remote boot image file, to the LOGIN directory, and to any default directory named in the workstation's login script.

Using Remote Reset with Multiple Servers

If you have multiple NetWare servers on your network, copy the remote boot image files onto each server that may come up as the remote boot workstation's default server.

Then, if the first default server isn't available, the station can boot from the next available server.

Using Multiple Remote Boot Image Files

For multiple workstations with different configurations to use Remote Reset, upload multiple remote boot image files into SYS:LOGIN.

Instead of the single NET$DOS.SYS file, create a separate remote boot image file for each workstation. Name the image files for each user (for example, FRED.SYS for user FRED).

Then, in the LOGIN directory, create a BOOTCONF.SYS file, which is a DOS text file that, for each station's network board, identifies the

- IPX external network number
- Node number
- Remote boot image filename (FRED.SYS)

See also the Novell Client documentation.

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 (Ri) attribute

A file system attribute that prevents any user from renaming the directory or file.

See also "Attributes."

Rename right

An object right that grants the right to change the name of an object, in effect changing the naming property.

See also “Rights.”

Replica

A copy of a Novell Directory partition.

See “Novell Directory replica.”

Resource tags

Operating system tags that keep track of NetWare server resources such as screens and allocated memory.

NLM programs request a resource from the NetWare server for each kind of resource they use and then give it a resource tag name.

NLM programs return resources when they no longer need them. When the NLM is unloaded, the resources are returned to the NetWare server.

Resource tags ensure that allocated resources are properly returned to the operating system upon termination of an NLM program.

Related utility: MONITOR in *Utilities Reference* .

Resources

The manageable components of a network, including

- Networking components, such as cabling, hubs, concentrators, adapters, and network boards
- Hardware components, such as servers, workstations, hard disks, and printers

- Major software components, such as the NetWare operating system and resulting network services (including file, mail, queue, and communication)
- Minor software components that are controlled by the operating system of its subsystems—protocols, gateways, LAN and disk drivers, etc.
- Data structures and other network resources such as volumes, queues, users, processes, security, etc.

Restore

A retrieval of data previously copied and backed up to a storage media. Perform a restore if data has been lost or corrupted since the backup.

See also “Backup” ; “Data set.”

Resynchronization

The process of returning SFT III servers to a mirrored (identical) state.

When both SFT III servers are restored to operation following a failure, they automatically resynchronize memory images and remirror disks.

The time it takes the servers to complete resynchronization depends on the amount of memory and the disk storage in each server. Server memory synchronization is much faster than disk remirroring because disk remirroring speed is limited by the disk channel.

Both servers—primary and secondary—continually poll each other so that each server is aware of its partner's state. Whenever an SFT III server is running in an unmirrored state, it searches for its partner.

As soon as it detects the presence of its partner on the other end of the mirrored server link, it automatically attempts to synchronize with the other server and return to a mirrored state.

Following a failure, SFT III tracks changes to the surviving server's disk and remirrors only the information that has changed. New data from the surviving server's disk is copied to the failed server's disk when the failed server is restored to operation.

Workstation and printer activity halts during memory synchronization, and workstations may appear to freeze for a few seconds. However, workstations are unaffected while the two servers' disks are remirrored because this process occurs in background mode.

Heavy network activity may slow down the remirroring process. Until disk remirroring is complete, the secondary server gets its disk data from the primary server. Thus, the secondary server is not fully operational until all disks are remirrored.

Reverse Address Resolution Protocol

(RARP) The process of determining the Internet address from a local data link address.

To communicate with a device on Ethernet, the router first must determine the 8-bit MAC or local data link address of that device. The process of determining the local data link address from an Internet address is called address resolution. RARP provides the reverse functionality.

See also "Address Resolution Protocol."

Rights

Qualities assigned to an object that control what the object can do with directories, files, or other objects. Creating, reading, and other operations can be done only if an object has rights to perform them.

Rights are granted to a specific directory, file, or object by *trustee assignments.* An object with a trustee assignment to a file, directory, or another object is a trustee of that file, directory, or object.

Within each object is a list of who has rights to the object and what rights the object has to other objects. This list is the ACL property of the object. (Files and directories contain similar information, but not an ACL.)

For example, to grant user JILL the right to delete a Printer object, go to the Printer object and make JILL a trustee; don't go to Jill and make the Printer object a trustee.

Directory Rights

Directory rights apply to the directory in the NetWare file system they are assigned to, as well as to all files and subdirectories in that directory (unless redefined at the file or subdirectory level).

Directory rights are a part of the file system. They aren't assigned to NDS objects. But, a User object can be granted Directory rights to a directory on a volume.

The following table describes directory rights.

Table 17-1 Directory Rights

Right	Description
Supervisor	Grants all rights to the directory, its files, and subdirectories. The Supervisor right can't be blocked by an Inherited Rights Filter. Users with this right can grant other users rights to the directory, its files, and subdirectories.
Read	Grants the right to open files in the directory and read the contents or run the programs.
Write	Grants the right to open and change the contents of files in the directory.
Create	Grants the right to create new files and subdirectories in the directory. If Create is the only right granted to a trustee for the directory, and no other rights are granted below the directory, a drop box directory is created. In a drop box directory, you can create a file and write to it. Once the file is closed, however, only a trustee with more rights than Create can see or update the file. You can copy files or subdirectories into the directory and assume ownership of them, but other users' rights are revoked.
Erase	Grants the right to delete the directory, its files, and subdirectories.
Modify	Grants the right to change the attributes or name of the directory and of its files and subdirectories, but does *not* grant the right to change the contents of them. (Changing the contents requires the Write right.)
File Scan	Grants the right to see the directory and its files with the DIR or NDIR command.
Access Control	Grants the right to change the trustee assignments and the Inherited Rights Filter of the directory and of its files and subdirectories.

File Rights

File rights apply only to the file they are assigned to. A trustee can also inherit rights to a file from the directory above the file.

The following table describes file rights.

Table 17-2File Rights

Right	Description
Supervisor	Grants all rights to the file. The Supervisor file right can't be blocked with an Inherited Rights Filter. Users who have this right can also grant other users any rights to the file and can change the file's Inherited Rights Filter.
Read	Grants the right to open and read the file.
Create	Grants the right create a file and to salvage a file after it has been deleted.
Write	Grants the right to open and write to an existing file.
Erase	Grants the right to erase (delete) the file.
Modify	Grants the right to change the attributes and name of the file, but does *not* grant the right to change its contents. (Changing the contents requires the Write right.)
File Scan	Grants the right to see the file with the NDIR directory command, including the directory structure from that file to the root directory.
Access Control	Grants the right to change the trustee assignments and the Inherited Rights Filter of the file.

Object Rights

Object rights apply to NDS objects. Object rights don't affect the properties of an object (see property rights later in this section). A trustee can inherit rights to an object from the object above it.

The following table describes object rights.

Table 17-3 Object Rights

Right	Description
Supervisor	Grants all access privileges. A trustee with the Supervisor object right also has unrestricted access to all properties. The Supervisor object right *can* be blocked by an Inherited Rights Filter below the object where the Supervisor right is granted.
Browse	Grants the right to see this object in the Directory tree. The name of the object is returned when a search is made that matches the object.
Create	Grants the right to create a new object below this object in the Directory tree. Rights are not defined for the new object. This right is only available on container objects because non-container objects can't have subordinates.
Delete	Grants the right to delete the object from the Directory tree. Objects that have subordinates can't be deleted (unless subordinates are deleted first).
Rename	Grants the right to change the name of the object, in effect changing the naming property. This changes the object's complete name.

Property Rights

Property rights apply to the properties of an NDS object. Rights can be assigned to all properties as a whole or to selected properties.

The following table describes property rights:

Table 17-4 Property Rights

Right	Description
Supervisor	Grants all rights to the property. The Supervisor property right can be blocked by an object's Inherited Rights Filter.
Compare	Grants the right to compare any value to a value of the property. With the compare right, an operation can return True or False, but you can't see the value of the property. The Read right includes the Compare right.
Read	Grants the right to read the values of the property. Compare is a subset of Read. If the Read right is given, compare operations are also allowed.
Write	Grants the right to add, change, or remove any values of the property. The Write right includes the Add or Delete Self right.
Add or Delete Self	Grants a trustee the right to add or remove *itself* as a value of the property. The trustee can't affect any other values of the property. This right is only meaningful for properties that contain object names as values, such as group membership lists or mailing lists. The Write right includes Add or Delete Self.

To grant directory or file rights to other objects, a trustee must have the Access Control right to a directory or file.

To grant object or property rights to other objects, a trustee must have the Write, Add or Delete Self, or Supervisor right to the ACL property of the object.

Rights are granted and revoked by creating trustee assignments with the RIGHTS, NETADMIN, or NetWare Administrator utilities.

Related utilities: NETADMIN , NetWare Administrator , and RIGHTS in *Utilities Reference* .

See also "Access Control List" ; "Security."

RIP (IPX)

(Router Information Protocol) A protocol that provides a way for routers to exchange routing information on a NetWare internetwork.

See "Router Information Protocol."

RIP (TCP/IP)

A distance vector internal gateway protocol for TCP/IP networks.

A TCP/IP Routing Information Protocol (RIP) router periodically broadcasts a routing update message that contains an entry for each network it can reach and the cost (distance) to that network. TCP/IP RIP routers listen to all TCP/IP RIP broadcast messages.

Each entry in a received routing update message is added to the routing table. The router that sent the routing update message is remembered as the next router (hop) on the route to the network in the entry.

If a router learns about two routes to a network, it keeps the one with the lower cost. Cost is defined in RIP in terms of hop count, or the number of routers along the path to the destination. TCP/IP RIP allows a maximum cost (hop count) of 15.

Once a route is learned, it must be refreshed at certain intervals. This is done to ensure that the route is still valid. TCP/IP RIP routers normally broadcast a routing update message containing known routes once every 30 seconds.

A timer is started when a route is learned from a routing update message. If a subsequent routing update message does not refresh the route within 180 seconds, the route is assumed to be unusable because of a network or node failure. The route is removed from the routing table.

See also “Router Information Protocol.”

RIP II (TCP/IP)

An enhancement to RIP that includes the subnetwork mask in its routes.

The lack of subnet mask information limits RIP to advertising only network routes, or requires RIP routers to make assumptions about the subnetwork mask. When RIP is used in a subnetted network, all subnets are usually required to use the same subnetwork mask.

RIP II can be used in network topologies requiring variable length subnet masks, and it is able to support subnet 0. RIP II can also authenticate routing message exchanges.

Not all RIP routers support RIP II.

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 “File system.”

Root object

An object in the Directory tree whose purpose is to provide a highest point to access different Country and Organization objects, and to allow trustee assignments granting rights to the entire Directory tree.

Country, Organization, and Alias objects can be created at the Root object.

The Root object is a place holder; it contains no information.

See also “Directory tree” ; “Object.”

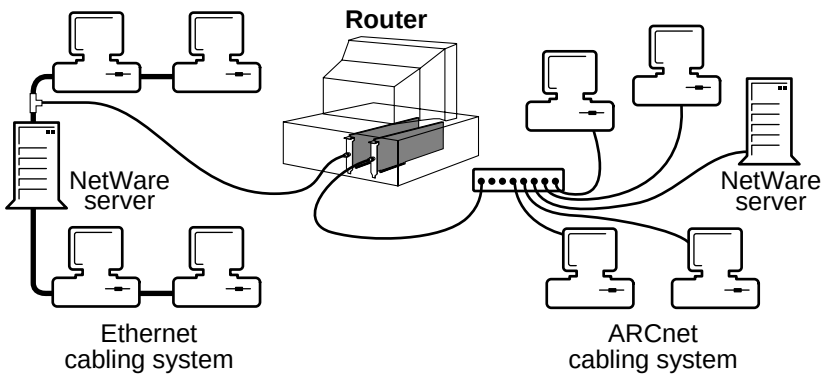
Router

A workstation or NetWare server running software that manages the exchange of information (in the form of data packets) between network cabling systems.

A NetWare router runs as part of a NetWare server. It connects separate network cabling topologies or separate networks by way of the server's NetWare operating system.

NetWare automatically routes IPX/SPX packets. However, NetWare is enabled for non-routing TCP/IP and AppleTalk protocols. To set your server to route TCP/IP and AppleTalk packets, use the INETCFG utility.

Figure 17-1
Router



NetWare Router versus Traditional Bridge

A NetWare router, unlike a traditional bridge, does more than just transfer data packets between networks that use the same communications protocol.

A NetWare router is intelligent. It not only passes packets of data between different cabling systems, but also routes the packets through the most efficient path.

A NetWare router can also connect cabling systems that use different kinds of transmission media and different addressing systems.

For example, a NetWare router can connect a network using the Ethernet addressing structure and RG/58 coaxial cable to another network using the ARCnet addressing structure and RG/62 coaxial cable.

Local versus Remote

When a router is used within the cable length limitations for its LAN drivers, it is a local router. If the router is connected beyond its driver limitations or through a modem, it is a remote router.

Router Information Protocol

(RIP) A protocol that provides a way for routers to exchange routing information on a NetWare internetwork.

RIP allows NetWare routers to create and maintain a database (or router table) of current internetwork routing information.

Workstations can query the nearest router to find the fastest route to a distant network by broadcasting a RIP request packet.

Routers send periodic RIP broadcast packets containing current routing information to keep all routers on the internetwork synchronized. Routers also send RIP update broadcasts whenever they detect a change in the internetwork configuration.

By default, a NetWare router sends RIP packets to each of its connected network segments every 60 seconds.

Routes that don't appear in these periodic broadcasts (because a router has failed) are *aged* . After a certain period of time (default: 3 minutes), routers delete the aged routes from their router tables.

To reduce traffic on lower bandwidth (X.25 and asynchronous) segments, network supervisors can configure routers to send only RIP updates rather than periodic RIP broadcasts over those segments.

However, turning off the periodic RIP broadcasts can cause inconsistencies on the internetwork. For example, if an unreliable segment loses a RIP update packet, routers on that segment broadcast old information.

INETCFG and FILTCFG allow network supervisors to configure RIP broadcasts for each network segment. To avoid inconsistencies in broadcast and aging intervals, all routers on the same network segment must have the same RIP configuration.

Related utilities: INETCFG and FILTCFG in *Utilities Reference* .

See also "Router" ; "Service Advertising Protocol."

RPL

(Remote Program Load) Technology based on the concept of storing an image of a bootable floppy disk on a NetWare volume.

See "Remote Program Load."

Chapter 18 S

Salvageable files

Files saved by NetWare, after being deleted by users, that can be salvaged (recovered).

Salvageable files are usually stored in the directory from which they were deleted. If the user deletes that directory, the file is saved in a DELETED.SAV directory located in the volume's root directory.

The user can view a list of deleted files in a directory and recover files by using the FILER utility. Recovered files contain information about who deleted the files and when they were deleted.

Deleted files are saved until the user deliberately purges them or until the NetWare server runs out of disk allocation blocks on the volume.

When the NetWare server runs out of blocks, it purges deleted files beginning with the files that were the first deleted.

Files and directories can also be purged as they are deleted. You can do this one of two ways:

- Use the SET command at the NetWare server to disable the salvageable file feature. This increases performance, but at the cost of losing the salvageable file feature.
- Set the Purge file system attribute. When a file is flagged with the Purge attribute, the file is purged when it is deleted.

  When a directory is flagged with the Purge attribute, any file in that directory is purged when the directory is deleted. Such files and directories can't be recovered with the FILER utility.

Related utility: FILER in *Utilities Reference* .

SAP

(Service Advertising Protocol) A protocol that provides a way for servers to advertise their services on a NetWare internetwork.

See “Service Advertising Protocol.”

SBACKUP

A backup engine that provides backup and restore capabilities.

See “Storage Management Services.”

Schema

The architecture that defines the types of NDS objects that are allowed and the properties associated with each object type.

Additional types of NDS objects and additional properties for existing objects can be defined by users with the Supervisor right to the [Root] object.

The default NDS objects and their properties cannot be deleted.

Each property in the schema can have any of the following flags, which cannot be modified:

- **DS_HIDDEN** Indicates that no user (even with the Supervisor right) can read or write to the property.
- **DS_READ_ONLY** Indicates that no user (even with the Supervisor right) can write to the property.
- **DS_PUBLIC_READ** or *DS_SERVER_READ* Indicates that the property can be read by any user, even if they are not authenticated. If this right is set on a property, you cannot stop access to the property, even with an Inherited Rights Filter or by assigning trustee rights.

See also “Object” ; “Inherited Rights Filter.”

SCSI bus

An interface that connects additional HBAs to controllers and hard disks.

When using a SCSI bus, make sure connected peripherals are properly terminated and addressed.

You can identify a SCSI bus by its 50-pin connector. (As opposed to an IDE bus, which has a 40-pin connector.)

See also “Hard disk.”

Search drive

A drive that the operating system searches when a requested file isn't found in the current directory.

Search drives are supported only from DOS workstations.

A search drive allows a user working in one directory to access an application or data file located in another directory.

See also “Drive mapping.”

Search modes

Methods of operation that specify how a program uses search drives when looking for a data file.

When an .EXE or .COM file requires an auxiliary file, it makes an open request through the operating system. The request might or might not specify the path to that file.

If a path is specified, the operating system searches that path. Otherwise, it only searches the default directory.

If the file isn't found, the NetWare shell uses the search mode of the executable file to determine if it should continue looking for the file in the search drives.

FLAG allows you to set the search mode for executable files individually, or you can set the shell's search mode in the NET.CFG file for the majority of your files.

The following table describes the types of search modes.

Mode	Description
0	The default setting for all executable files. The executable file looks for instructions in the NET.CFG file.
1	The executable file searches the path specified in the file itself. If there is no path, the file searches the default directory and then all search drives.
2	The executable file searches the path specified in the file itself. If there is no path, the file searches only the default directory.
3	The executable file searches the path specified in the file itself. If there is no path, the file searches the default directory; then if the open request is read-only, the file searches the search drives.
4	Reserved.
5	The executable file searches the path specified first and then all search drives. If there is no path, the file searches the default directory and then all search drives.
6	Reserved.
7	The executable file searches the path specified first. If the open request is read only, the file searches the search drives. If there is no path, the file searches the default directory and then all search drives.

For example, if you assign an executable file mode 2, it won't use search drives.

If you assign mode 5, the executable file can use search drives to find a data file if the file isn't found in the first directory the executable file looks in.

Related utility: FLAG in *Utilities Reference* .

Secondary server

The SFT III server that is activated after the primary server.

The secondary server receives a mirrored copy of the memory and disk from the primary server (the first server activated). In addition to mirroring the primary server, the secondary server provides split seeks. SFT III splits multiple read requests between the two servers' disks for faster disk reads.

Though it cannot be used to do additional work (because it uses all of its CPU cycles keeping up with the primary server), the secondary server acts as a router for the local network segments to which it is directly attached. If both SFT III servers are on the same network segment, the secondary server doesn't do any routing.

If a secondary server acting as a router goes down, so does the routing. The primary server doesn't take over the routing that the secondary server provided.

Either SFT III server may function as primary or secondary, depending on the state of the system. You cannot permanently designate which server is primary or secondary; system failure determines each server's role. When the primary server fails, the secondary server becomes the new primary server. When the failed server is restored, it becomes the new secondary server.

Secondary time server

A server that obtains the time from a Single Reference, Primary, or Reference time server and provides the time to workstations.

See "Time synchronization."

Security

Elements that control access to the network or to specific information on the network. Six categories of security features are

- **Login security** Controls which users can access the network.
- **Trustees** Designate which users can access directories, files, or objects.
- **Rights** Determine the level of access for each trustee.
- **Inheritance** Passes rights from higher to lower levels.
- **Attributes** Describe characteristics of directories and files.

- **Effective rights** List a user's actual rights to a directory, file, or object (including explicitly granted rights and inherited rights).

Login Security

The LOGIN command controls who can access the network by determining if a valid user is attempting to log in.

A person must know the User object's name and the correct password (if required) to log in.

The network supervisor establishes this login security by creating a User object in NDS and by then assigning values to the properties of that user. Those values determine how the user can access the network.

A User object's properties affect when a user can log in, which workstations a user can log in to, when the user's account is disabled, etc.

Passwords aren't required, but they should be used. Without one, an intruder can access the network with only a user's name. Don't use family or pet names as passwords; they are easily guessed by an intruder.

Passwords are encrypted and are never displayed on the monitor or transmitted across the network. The password authenticates every action of a user.

You can assign and change passwords, or you can assign initial passwords and allow users to change them. To increase login security, consider requiring these password options:

- **Minimum password length**. Prevents the use of passwords that might be easily guessed. (Default: 5 characters.)

- **Periodic password change**. Prevents the user from keeping a password indefinitely. (Default: every 40 days.)

- **Unique password**. Prevents alternating between a few favorite passwords. The server remembers and rejects the use of the eight passwords most recently used for one day or longer.

Trustees

A trustee is a User or Group object that has been granted access to a directory, file, or object. Access is granted through a *trustee assignment.*

Any object with sufficient rights can make trustee assignments with the RIGHTS, NETADMIN, or NetWare Administrator utilities.

- **Trustee list**. Each directory, file, and object has a list of trustee assignments, called a *trustee list* , that specifies who can access that directory, file, or object.

  An object's trustee list is stored in the object's ACL property.

- **Trustees of groups**. For several users to access a directory, file, or object, a trustee assignment is required for each user. Rather than make trustee assignments for each user individually, create a Group object, include the users in the group, and then grant access for the group with one trustee assignment.

- **[Public] trustee**. [Public] is a special trustee that can be added to an object, directory or file.

  The rights assigned to [Public] are effective for anyone who has no rights to the file, directory, or object.

Rights

Rights determine the type of access a trustee has to a directory, file, or object. For example, if a trustee assignment grants the Create right to a directory, a trustee can create files in the directory.

A trustee assignment grants one object rights to another object. By default, every trustee assignment includes the Browse object right and the Read right for all properties.

Rights are granted within the object a trustee has rights to, not within the trustee object.

For example, to grant JILL the right to delete a Printer object, make JILL a trustee of the Printer object and include the delete right in her assignment—don't make the Printer object a trustee of JILL.

Because directories, files, and objects contain such different information, the rights that control access to each are different.

Rights to directories and files and to other objects are controlled in different sections of the utilities.

There are four kinds of rights in NetWare 4:

- Directory rights control what a trustee can do with a directory.

  Directory rights also apply to files in the directory *if* file rights aren't granted and *if* the file's Inherited Rights Filter doesn't block the directory rights.

- File rights control what a trustee can do with a file.

- Object rights control what a trustee can do with an object.

  These rights control the object as a single piece in the directory tree, but don't allow access to information stored within that object (except the Supervisor object right, which also allows access to an object's properties).

- Property rights control a trustee's access to information stored within the object—that is, the information stored in the object's properties.

  Each object type has a different set of properties.

  Property rights can be managed in NETADMIN or NetWare Administrator using the All Properties or the Selected Properties option.

  Rights assigned using All Properties affect every property equally. Rights assigned using Selected Properties affect individual properties only.

To grant directory or file rights to other objects, an object must have the Access Control right to that directory or file. To grant object or property rights, a user must have the Write right to the object's ACL property.

For a list and description of all rights, see “Rights.”

Related utilities: RIGHTS , NETADMIN , and NetWare Administrator in *Utilities Reference* .

Inheritance

Creating a trustee assignment for every user and for every directory, file, and object would be a huge job. *Inheritance* simplifies the task.

Through inheritance, rights granted in a trustee assignment apply to objects, directories, and files below the assignment. Rights change if another trustee assignment is made or if the rights are blocked by an IRF.

Inheritance applies both to directories and files on a volume and to objects in the Directory tree.

For directories and files, all access rights are inherited. For objects, only object rights and rights assigned with All Properties are inherited. Rights to specific properties of an object can't be inherited.

Rights assigned to NDS objects do not affect file system rights. For example, object rights assigned to a Volume object do no affect the directory and file system rights in the physical volume represented by that Volume object.

However, one exception exists: Any trustee with the Supervisor right to a NetWare Server object or to that object's ACL property is granted the Supervisor right to any physical volume attached to that server.

An IRF stops rights from being inherited. An IRF has the same set of possible rights as a trustee assignment, but instead of granting rights, it revokes rights.

Every directory, file, and object has an IRF. With this filter, you can grant access more freely at the top of the object tree or volume, then filter out rights in sensitive areas.

With all rights in sensitive areas blocked by an IRF, only users with a trustee assignment in those areas have access. No one can inherit rights blocked by an IRF. (See "Inherited Rights Filter.")

Important

Be careful not to block everyone's rights to an object with an Inherited Rights Filter, leaving no one with access to part of the Directory tree.The utilities don't allow you to block the Supervisor object right unless a trustee already has the Supervisor object right at that point. But you could still delete the trustee object, making the trustee assignment invalid and cutting off access to that part of the Directory tree.

Attributes

Attributes (also called *flags*) describe the characteristics of a directory or file and tell NetWare what actions are allowed, and in a few cases, what actions have been performed. They aren't used for objects.

NetWare reads the attributes you set (for example, to compress, back up, or not allow deletion of a file) and sets other attributes to tell you what has been done (for example, that a file has been compressed, migrated, or indexed).

Attributes are separate from rights. Attributes aren't inherited, and if an attribute indicates that a file can't be deleted, not even a supervisor can delete it without first changing the attribute.

To change the attributes of a directory or file, an object must be granted the Modify right in a trustee assignment for the directory or file. (See "Attributes.")

Related utilities: FLAG , FILER , NETADMIN , and NetWare Administrator in *Utilities Reference* .

Effective Rights

Effective rights are the rights that a user actually has to a directory, file, or object.

NetWare calculates your effective rights to a directory, file, or object whenever you take an action.

Effective rights to a file or directory are determined by

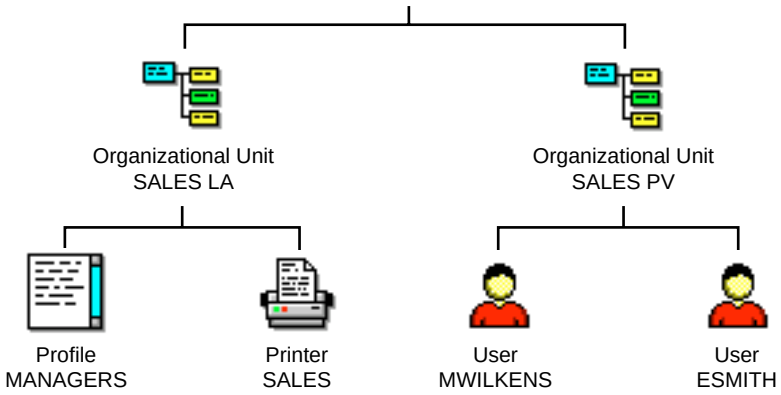
- An object's trustee assignments to the directory or file
- Inherited rights from an object's trustee assignments to parent directories
- Trustee assignments of Group objects that a User object belongs to
- Trustee assignments of objects listed in a User object's Security Equal To list

If a user has a trustee assignment to a directory on a given level in the file system, and also one on a higher level, the current trustee assignment overrides the higher one.

However, trustee assignments to a group are added to individual user trustee assignments.

Effective rights to an object are shown in the following figure.

Figure 18-1
Effective Rights



In the previous figure, MWILKENS' effective rights to access the MANAGERS profile can come from

- Trustee assignments on MANAGERS that list MWILKENS (explicit rights are granted)
- Trustee assignments on MANAGERS that list SALES PV (inherited from the trustee's container)
- Trustee assignments on SALES LA that list MWILKENS (inherited from the object's container)

  Rights must pass through MANAGERS' IRF before becoming effective.
- Trustee assignments on SALES LA that list SALES PV (inherited from object's container and trustee's container)

  Rights must pass through MANAGERS' IRF before becoming effective.
- Trustee assignments to any Group object that MWILKENS is a member of (only valid when the object requesting rights is a User object)
- Trustee assignments to any object listed in MWILKENS' Security Equal To list (only valid when the object requesting rights is a User object)

If MWILKENS has a trustee assignment to SALES LA and to MANAGERS, the Trustee assignment on MANAGERS overrides the trustee assignment on SALES LA.

Trustee assignments to groups, however, are added to previous trustee assignments for User objects.

No rights are granted by default. They must be granted by a trustee assignment at some point.

The Supervisor right can be filtered for object and property rights, but can't be filtered for file system rights.

See also “Attributes” ; “Effective rights” ; “Inherited Rights Filter” ; “Rights” ; “Security Equal To” ; “Trustee.”

Security Equal To

A property of every User object that lists other objects. The user is granted all rights that any object (such as User, Group, or Printer objects) in that list is granted, both to objects and to files and directories.

Use the Security Equal To property to give a user *temporary* access to the same information or rights another user has access to.

When a user is added to the membership list of a Group object or the occupant list of an Organizational Role object, the Group or Organizational Role is listed in that user's "Security Equal To" list.

By using a security equal, you avoid having to review the whole directory structure and determine which rights need to be assigned to which directories, files, and objects.

However, if an object in a user's "Security Equal To" list is deleted from NDS, the user no longer has the rights granted through that object.

Important

Use the Security Equal To property with caution. If users have rights to add to their own "Security Equal To" list, they could add the name of a network supervisor and change anything on the network.

Be careful when granting the Write or Supervisor property right to this property and consider blocking it in the Inherited Rights Filter of each User object. This way, only network supervisors and those granted specific rights to this property can add to the list.

Users who manage other users should be granted the Write right to this property. This allows user account managers to make users security equal to other users that they manage.

Every object is security equal to all container objects that are part of its complete name. Because of this, you can make a container a trustee.

Every object in that container has the rights that are granted to the container, through the Security Equal To property. However, none of these containers are listed in a users "Security Equal To" list.

The Security Equal To property is not transitive; that is, if TOM is security equal to JILL, and JILL is security equal to BOB, TOM is not security equal to BOB through JILL. The Security Equal To property only grants TOM those rights that JILL is explicitly granted.

To add an object to a user's "Security Equal To" list, you must have at least the Write property right to the ACL property of the object you want to add to the list. You don't need rights to the Security Equal property of the user; only the Browse object right.

In networks containing confidential data that only selected users have access to, take care that you don't inadvertently give a user access to restricted information.

Related utilities: NETADMIN and NetWare Administrator in *Utilities Reference* .

See also "User object."

Semaphore

An integer value used to coordinate activities of both programs and processes to prevent data corruption in multiprocessor environments.

Semaphores are used to synchronize interprocess communication by ensuring that certain event sequences do or do not occur.

Another use of semaphores is a binary semaphore, which controls the use of shared resources by enforcing mutually exclusive access to those resources.

For example, access to a shared file could be controlled by using a binary semaphore. If the file is not in use, the semaphore value is 1 and the file is

available. If the file is in use, the semaphore value is 0. While the semaphore value is 0, no other process can access the file.

Semaphores can also allow a limited number of users access to a resource, such as to network applications with limited-user licenses. When the specified number is reached, the semaphore denies access to additional users.

NetWare supervisors never see or change a semaphore's value in NetWare. NLM developers use semaphores extensively.

If you receive system messages that refer to semaphores, it is likely that the message is referring to shared resource management issues.

Serial communication

The transmission of data between devices over a single line, one bit at a time.

NetWare uses the RS-232 serial communication standard to send information to serial printers, remote workstations, remote routers, and asynchronous communication servers.

The RS-232 standard, developed by the Electronic Industries Association (EIA), enhances 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 received.

For example, a printer can be thought of as a system that transforms the binary data it receives from the computer into 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* 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 1200, 2400, 4800, and 9600. The higher the number, the greater the number of signal changes and, therefore, the faster the transmission.

- *Character length* The number of data bits used to form a character.

  The standard ASCII character set (including letters, numbers, and punctuation) consists of 128 characters and requires a character length of 7 bits for transmissions.

  Extended character sets (containing line drawings or the foreign characters used in IBM's extended character set) contain an additional 128 characters and require a character length of 8 bits.

- *Parity* A method of checking for errors in transmitted data. You can set parity to even or odd, or not use parity at all.

  Serial communication sends information in a stream of bits called a *frame* . Each frame consists of start bits, data bits, an optional parity bit, and stop bits.

  The parity bit is set to 0 or 1 so that the sum of the data bits is even or odd. Upon reception, each transmitted frame is checked to ensure that the parity is still even or odd.

  If it is incorrect (because a bit was changed during transmission), the communications software determines that a transmission error has occurred and can request that the data be retransmitted.

  The following table shows examples of parity checking:

Table 18-1

Character length	Sample bits	Even parity	Odd parity
7 data bits	0010110	00101101	00101100
7 data bits	1110111	11101110	11101111
8 data bits	10001000	100010000	100010001
8 data bits	11011111	110111111	110111110

- **Stop bit** A special signal that indicates the end of that character. Today's modems are fast enough that the stop bit is always set to 1. Slower modems require two stop bits.

- **XON/XOFF** One of many methods that prevents the sending system from transmitting data faster than the receiving system can accept it.

Serial port

A port that allows data to be transmitted asynchronously, one bit at a time. Typically, serial ports are used for modems or serial printers.

On IBM PC-compatible computers, COM1 and COM2 are asynchronous serial ports.

Server

A computer in a network shared by multiple users.

NetWare server A computer running the NetWare operating system software. (See “NetWare server.”)

Print server A computer that takes print jobs out of a print queue and sends them to a network printer. (See “Print server.”)

Server console

The monitor and keyboard where you view and control NetWare server activity. You can

- View network traffic
- Send messages
- Set configuration parameters
- Shut down the server
- Load and unload NLM programs

Many server console tasks are done in MONITOR and PSERVER.

MONITOR allows you to view server and memory use, connections, and many disk and network statistics. PSERVER allows you to control active printers on the network.

Note

RCONSOLE.EXE allows a workstation to function as a server console.

Be aware of the following console security issues:

- Unauthorized access of the server console. Control keyboard access by requiring the use of a password. (See Securing the Server Console in *Supervising the Network* .)

  Use the SECURE CONSOLE command to secure your console against breaches of security. (See SECURE CONSOLE in *Utilities Reference* .)

- Software tampering. An expert could use the built-in debugger to disable or bypass the security system. To prevent this, use SECURE CONSOLE.

- Hardware tampering. Keep your server in a secure location. An intruder could disable the power-on password or remove hard disks to access data.

Server mirroring

An SFT III configuration that provides a secondary, identical server to immediately take over network operations when the primary server fails.

Server mirroring requires two similarly configured network servers. They should be evenly matched in terms of CPU speed, memory, and storage capacity.

The servers are not required to be identical in terms of processor type, processor revision level, or clock speed. However, identical servers are recommended for better performance. If the two servers are unequal, then SFT III performs at the speed of the slower server.

The servers must be directly connected by a mirrored server link. SFT III servers can reside on different network segments, as long as they share a dedicated mirrored server link and each can reach the other server on the internetwork.

Service Advertising Protocol

(SAP) A protocol that provides a way for servers to advertise their services on a NetWare internetwork.

Servers advertise their services with SAP, allowing routers to create and maintain a database of current internetwork server information.

Routers send periodic SAP broadcasts to keep all routers on the internetwork synchronized. Routers also send SAP update broadcasts whenever they detect a change in the internetwork configuration.

Workstations can query the network to find a server by broadcasting SAP request packets. When a workstation logs in to a network, it broadcasts a Get Nearest Server SAP request and attaches to the first server that replies.

To keep workstations from attaching to a server, network supervisors can turn off the Get Nearest Server SAP option.

By default, a NetWare router sends SAP packets to each of its connected network segments every 60 seconds.

With time synchronization, Single reference and Primary time servers advertise their services using SAP. Secondary time servers don't advertise their services.

Related utilities: MONITOR , INETCFG , and TIMESYNC in *Utilities Reference* .

See also "Router" ; "Router Information Protocol."

SFT

(System Fault Tolerance) A means of protecting data by providing procedures that allow you to recover from hardware failures.

There are three levels of SFT: Hot Fix; Disk mirroring or duplexing; Server mirroring.

See "System Fault Tolerance."

Shareable (Sh) attribute

A file system attribute that allows a file to be accessed by more than one user at a time.

See also “Attributes.”

Short machine type

A four-letter (or less) name representing a brand of DOS workstations. The short machine type is similar to the long machine type, except the short machine type is used specifically with overlay files.

Files using the short machine type include the IBM$RUN.OVL file for windowing utilities and the CMPQ$RUN.OVL file that uses a default black-and-white color palette for NetWare menus.

The short machine type is set in the NET.CFG file, using the SHORT MACHINE TYPE parameter. The default is IBM.

The short machine type can be accessed in login scripts, using the %SMACHINE identifier variable.

See also “Login scripts” ; “Long machine type.”

SIDF

(System Independent Data Format) The format standard SBACKUP uses. All data backed up using SBACKUP can be read by other backup applications that read and write SIDF.

Simple Network Management Protocol

(SNMP) An industry-standard protocol that specifies a format for collecting network management data.

With Desktop SNMP services, Novell Client workstations can send status information to an SNMP management program running on an IPX or TCP/IP network.

Desktop SNMP services can be managed using NMS™ software, industry-standard SNMP management consoles, or other third-party management systems.

Community Names and Types

Desktop SNMP and other SNMP entities use community names and types to provide access control. Desktop SNMP provides default community names for the monitor and control communities, as well as default community types used for traps.

Desktop SNMP supports the following three communities, as described in the following table:

Name	Explanation
Control community	Describes the read/write community (the community that is allowed to do SET operations).
Monitor community	Describes the read-only community (the community that is allowed to do GET and GET NEXT operations).
Trap community	Describes the community name used for traps.

The community name contained in a request message from an SNMP management station must match the name expected by Desktop SNMP.

A community name can be any ASCII string, up to 32 characters in length. It cannot include space, tab, open square bracket ([), equal sign (=), colon (:), semicolon (;), single quotation mark (), or number sign (#).

Important

Community name strings are case-sensitive. Always enclose the community name string in quotation marks.

Management Information Base (MIB-II) Support

Desktop SNMP automatically supports three MIB-II groups:

- System and SNMP groups
- Interface group

- TCP/IP groups (except interface, system, and SNMP, and EGP and transmission, which are not supported)

Single Reference time server

A server that provides time to Secondary time servers and to workstations. The Single Reference time server is the sole source of time on the network.

See also “Time synchronization.”

Small Computer Systems Interface

(SCSI) An industry standard that sets guidelines for connecting peripheral devices and their controllers to a microprocessor.

SMDR

(Storage Management Data Requester) Passes commands and information between SBACKUP and Target Service Agents.

See “Storage Management Data Requester.”

SMS

(Storage Management Services) A combination of related services that allow data to be stored and retrieved.

See “Storage Management Services.”

SMSDI

(SMS Storage Device Interface) A set of routines that allows SBACKUP to access various storage devices and media.

See “SMS Storage Device Interface.”

SMS Storage Device Interface

(SMSDI) A set of routines that allows SBACKUP to access various storage devices and media.

If more than one storage device is attached to the host, the SMSDI sends SBACKUP a list of storage devices and media, each labeled Available or Unavailable.

SBACKUP displays this list so you can select an available device to store backup data on.

If a storage device is unavailable, it is being used by another application. Such a device remains unavailable until the application gives it up, or until the application is exited.

See also “Backup” ; “Backup hosts and targets” ; “Media Manager” ; “Storage Management Services.”

SNA

(System Network Architecture) IBM's proprietary networking architecture, was first introduced in 1974.

See “System Network Architecture.”

SNMP

(Simple Network Management Protocol) An industry standard protocol that specifies a format for collecting network management data.

See “Simple Network Management Protocol.”

Socket

The part of an IPX internetwork address, within a network node, that represents the destination of an IPX packet.

Some sockets are reserved by Novell for specific applications. For example, IPX delivers all NCP request packets to socket 451h.

Third-party developers can also reserve socket numbers for specific purposes by registering those numbers with Novell.

The following table lists key socket numbers reserved by Novell:

Socket	Process
451h	NCP
452h	SAP
453h	RIP
455h	NetBIOS
456h	Diagnostics
8063h	Novell Virtual Terminal (NVT)
4000-6000h	Temporary sockets used for interaction with NetWare servers and other network communications

See also “IPX internetwork address.”

Source routing

A method used by IBM to route data across source-routing bridges. NetWare source routing programs allow an IBM token ring network bridge to forward NetWare packets (or frames).

IBM bridges can be configured as either single-route broadcast or all-routes broadcast. (Default: single-route broadcast.)

- *Single-route broadcasting*. Only designated single-route bridges pass the packet and only one copy of the packet arrives on each ring in the network.

  Single-route bridges can transmit single-route, all-routes, and specifically-routed 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 bridges in the network.

All-routes bridges pass both all-routes broadcasts and specifically-routed packets.

To support IBM hardware and applications, Novell provides ROUTE.NLM for the NetWare server and ROUTE.COM for DOS workstations.

These drivers allow users running NetWare 4 to communicate across IBM Token Ring network bridges. They also allow IBM applications that require source routing support to run unmodified on NetWare networks.

Parameters for ROUTE.NLM determine which packets are broadcast as all-routes packets or as single-route packets.

At the workstation, ROUTE.COM determines the type of packets the workstation broadcasts.

Add the command to load ROUTE.COM after LANSUP.COM or TOKEN.COM, but before the protocol stack (for example, IPXODI.COM).

Source server

The server from which you migrate data files, bindery files, and other information to a NetWare 4 destination server during upgrade.

See also “Destination server.”

Sparse file

A file with at least one empty block. (NetWare won't write any block that is completely empty.)

Databases often create sparse files.

For example, suppose the disk allocation block size for volume VOL1: is 4 KB. Also suppose that a database opens a new file, seeks out the 1,048,576th byte, writes five bytes, and closes the file.

An inefficient operating system would save the entire file to disk.The file would be comprised of 256 zero-filled disk allocation blocks (the first 1 MB) and one more disk allocation block with five bytes of data and 4,091 zeros. This method would waste 1 MB of disk space.

However, NetWare writes only the last block to disk, saving time and disk space.

Sparse files aren't limited to large files. If a two-block file is created and the first block is empty, the operating system treats the file as a sparse file.

If a program tries to read from a file's empty blocks, the operating system generates and returns zeros.

The NetWare NCOPY command doesn't copy sparse files automatically. NCOPY has a /f option that forces the operating system to copy sparse files.

SPX

(Sequenced Packet Exchange) A NetWare DOS Requester module that enhances the IPX protocol by supervising data sent out across the network.

SPX verifies and acknowledges successful packet delivery to any network destination by requesting a verification from the destination that the data was received.

The SPX verification must include a value that matches the value calculated from the data before transmission. By comparing these values, SPX ensures not only that the data packet made it to the destination, but that it arrived intact.

SPX can track data transmissions consisting of a series of separate packets. If an acknowledgment request brings no response within a specified time, SPX retransmits it.

After a reasonable number of retransmissions fail to return a positive acknowledgment, SPX assumes the connection has failed and warns the operator of the failure.

SPX is derived from Novell IPX using the Xerox Packet Protocol.

See also “NetWare DOS Requester” ; “NetWare user tools.”

STARTUP.NCF

A NetWare server boot file that loads the NetWare server's disk driver and name spaces and some SET parameters.

See also “Boot files.”

Station

Usually a shortened form of *workstation* , but can also be a server, router, printer, fax machine, or any computer device connected to a network by a network board and a communication medium.

Station address

A number that uniquely identifies a network board; usually referred to as the *node number.*

See “Node number.”

Stop bit

A signal that indicates the end of a character.

See also “Serial communication.”

Storage device

A device used to back up data from a server or workstation. An example of a storage device is an external tape drive that backs up data from a hard disk to magnetic tape.

Storage Management Data Requester

(SMDR) Passes commands and information between SBACKUP and Target Service Agents.

See also “Storage Management Services.”

Storage Management Services

(SMS) Services that allow data to be backed up and restored. SMS is independent of backup/restore hardware and file systems (such as DOS, MS Windows, or UNIX).

SMS Architecture

NetWare provides the following SMS-compliant NLM programs and other software modules that run on servers:

- **SBACKUP** is a backup engine that provides backup and restore capabilities.
- **SMDR (Storage Management Data Requester)** passes commands and information between SBACKUP and Target Service Agents.
- **SMSDI (SMS Storage Device Interface)** passes commands and information between SBACKUP and the storage devices and media.
- **Device drivers (IDE.DSK, TAPEDAI.DSK, AHAnnnn.DSK)** control the mechanical operation of storage devices and media by acting on commands passed from SBACKUP through the SMSDI.
- **NetWare Server Target Service Agents (such as TSA410)** pass requests for data (generated within SBACKUP) to the NetWare server where the data resides and then return requested data through the SMDR to SBACKUP.
- **Database Target Service Agents (such as TSANDS)** pass commands and data between the host server (where SBACKUP resides) and the database where the data to be backed up resides, then return the requested data through the SMDR to SBACKUP.
- **Workstation Target Service Agents (such as TSADOS)** pass commands and data between the host server (where SBACKUP resides) and the station where the data to be backed up resides, then return the requested data through the SMDR to SBACKUP.
- **Workstation Manager (WSMAN)** receives I am here messages from stations available to be backed up. It keeps the names of these stations in an internal list.

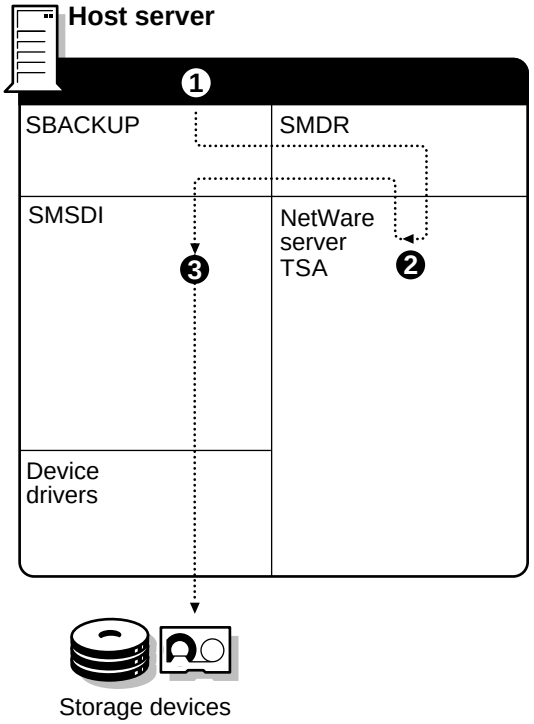
Although all SMS software modules are loaded on the host server, all modules aren't used in all backups.

See also Backing Up and Restoring Data in *Supervising the Network* .

Backing Up a Host Server

The following figure shows a simplified diagram of backing up a host server:

Figure 18-2
Backing Up a Host Server



The numbered portions in the preceding diagram are explained in the following list:

1. From the host server command line, the network supervisor initiates SBACKUP, which uses SMDR to access the NetWare server Target Service Agent.

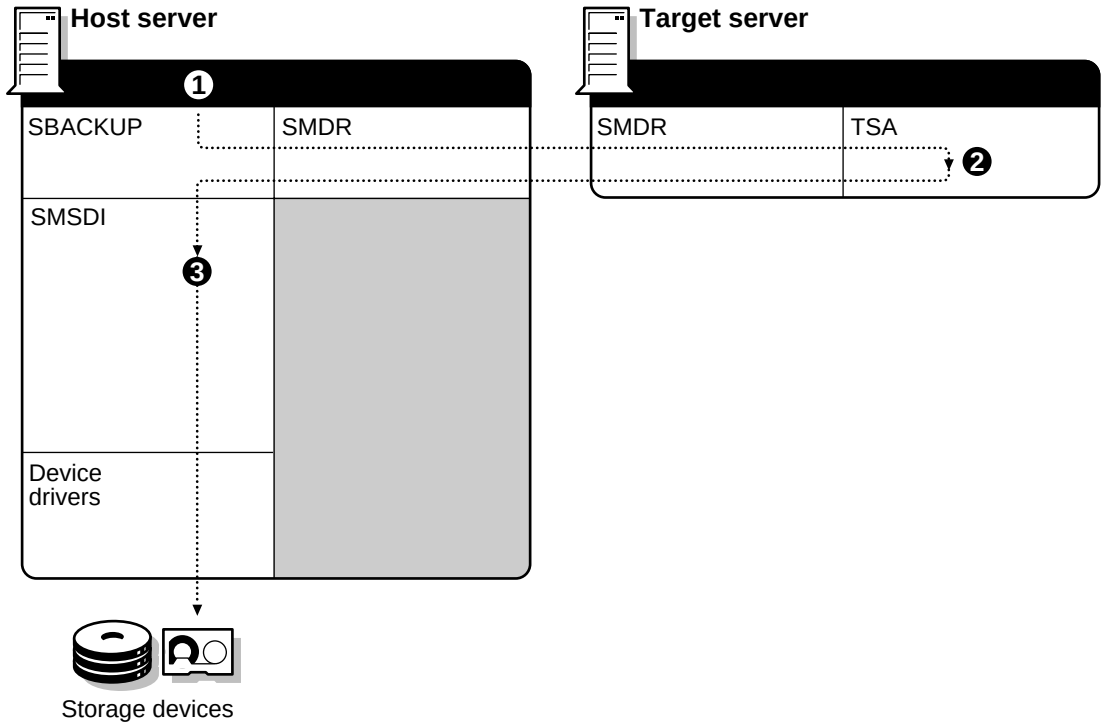
2. The server Target Service Agent (such as TSA410.NLM and TSA312.NLM) obtains the requested data, then passes it through the SMDR to SBACKUP, which passes it on to the SMSDI.

3. The SMSDI uses device drivers to send the data to the selected device and media for storage.

Backing Up a Target Server

The following figure shows a simplified diagram of backing up a target server (any server other than the host):

Figure 18-3
Backing Up a Target Server



The numbered portions in the preceding diagram are explained in the following list:

1. From the host server command line, the network supervisor initiates SBACKUP. SBACKUP uses the SMDR to access the Target Service Agent on the target server.

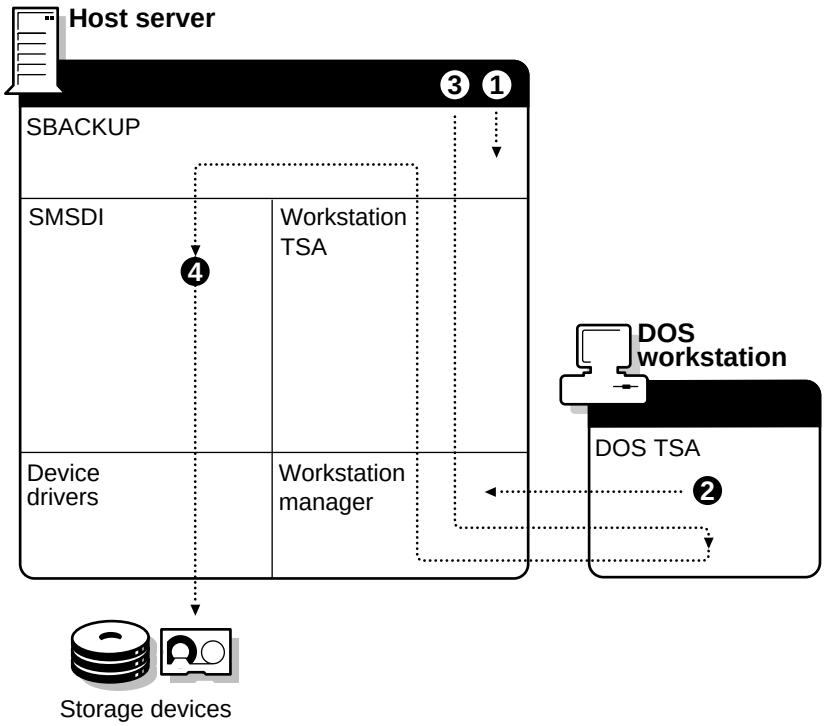
2. The Target Service Agent on the target (such as TSA312.NLM) obtains the requested data, then passes it through SMDR to SBACKUP, which passes it on to the SMSDI.

3. The SMSDI uses device drivers to send the data to the selected device and media for storage.

Backing Up a DOS Workstation

The following figure shows a DOS workstation backup:

Figure 18-4
Backing Up a DOS Workstation



The numbered portions in the preceding diagram are explained in the following list.

1. From the host server command line, the network supervisor initiates SBACKUP.

2. When the DOS Target Service Agent is loaded on the workstation, the DOS Target Service Agent contacts the Workstation Manager on the host server.

Important

The Workstation Manager keeps an internal list of all Target Service Agents that have contacted it. By implication, this is a list of workstations that have their Target Service Agent loaded.

3. SBACKUP uses the workstation Target Service Agent to access the Workstation Manager, which, in turn, obtains the data for the backup from the DOS Target Service Agent (TSASMS.COM) and returns it to SBACKUP, which passes it on to the SMSDI.

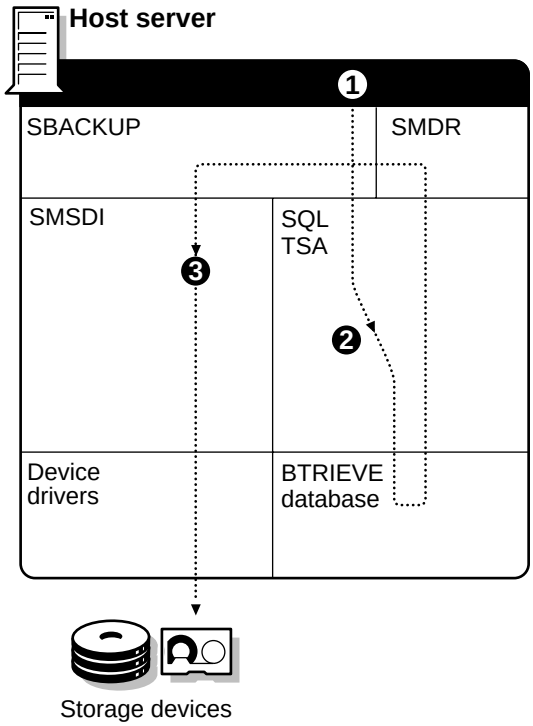
4. The SMSDI uses device drivers to send the data to the selected device and media for storage.

Backing Up a Btrieve Database

The following figure shows a simplified diagram of backing up a Btrieve database:

Figure 18-5

Backing Up a Btrieve Database



The numbered portions in the preceding diagram are explained in the following list.

1. From the host server command line, the network supervisor initiates SBACKUP, which uses the SQL Target Service Agent to access the Btrieve database (or databases) to obtain the data for the backup.

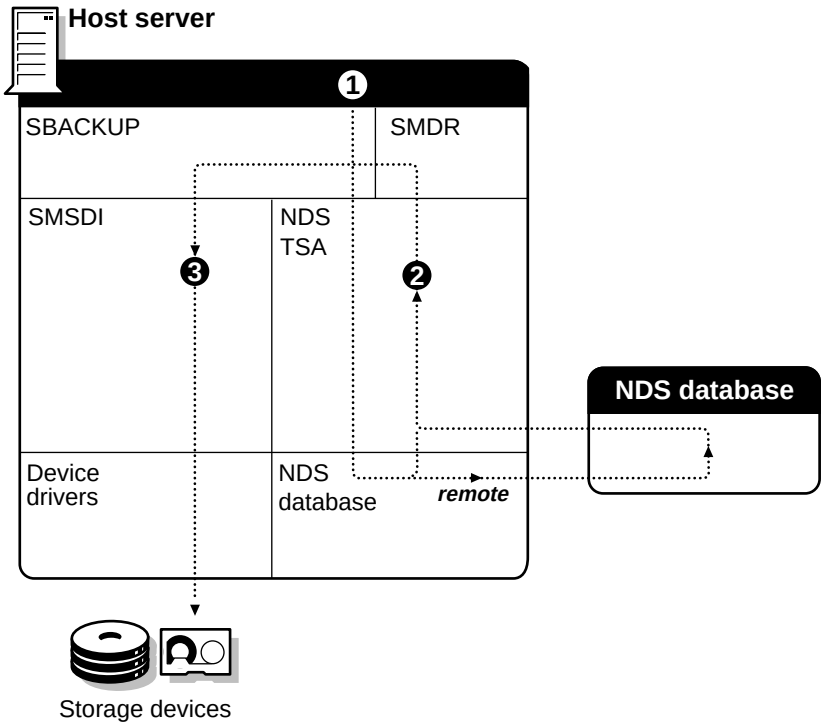
2. The SQL Target Service Agent (TSASQL) obtains the requested data from the database and passes it through the SMDR to SBACKUP, which passes the requested data to the SMSDI.

3. The SMSDI receives the data for storage from SBACKUP and uses device drivers to send the data to the selected device and media for storage.

Backing Up a Novell Directory Services Database

The following figure shows a simplified diagram of backing up a Novell Directory Services database:

Figure 18-6
Backing Up a Novell Directory Services Database



The numbered portions in the preceding diagram are explained in the following list.

1. From the host server command line, the network supervisor initiates SBACKUP, which uses the NDS Target Service Agent to access the NDS database (or databases) to obtain the data for the backup.

Note

An NDS database can be located on a local or remote server, or both, or on several servers. SBACKUP can back up the database regardless of where it is located.

2. The NDS Target Service Agent (TSANDS.NLM) obtains the requested data from the NDS database and passes it through the SMDR to SBACKUP, which sends it on to the SMSDI.

3. The SMSDI receives the data for storage from SBACKUP and uses device drivers to send the data to the selected device and media for storage.

See also “Backup hosts and targets” ; “Novell Directory database” ; “NetWare Loadable Module” ; “Storage Management Services” ; “Target Service Agent.”

STREAMS

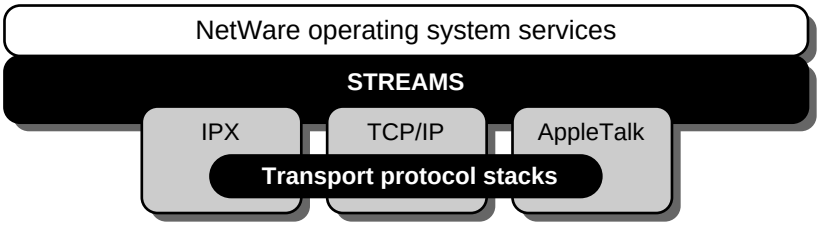
An NLM program that provides a common interface between NetWare and transport protocols such as IPX/SPX, TCP/IP, SNA, and OSI that need to deliver data and requests to NetWare for processing.

By making the transport protocol transparent to the network operating system, STREAMSTM allows services to be provided across the network, regardless of the transport protocols used.

Network managers can install the protocols of their choice or change the protocols used without affecting the level of services delivered to the user, if the applications support multiple protocols.

The relationship between STREAMS and the transport protocol stacks is illustrated in the following figure:

Figure 18-7
STREAMS Structure



Subdirectory

A directory below another in the file system structure. For example, in SYS:ACCTS\RECEIVE, RECEIVE is a subdirectory of SYS:ACCTS.

See also “File system.”

Subnetwork mask

Indicates how the host portion of the IP address is divided into subnetwork addresses and local host address portions.

The network mask is a 32-bit number with all ones for all network and subnetwork address portions of the complete IP address, and all zeros for host address portions.

With a 16-bit Class B IP network address, a 4-bit subnetwork address, and a 12-bit host address, the subnetwork mask consists of 20 ones and 12 zeros. In essence, a subnetwork mask locally extends the network address portion of an IP address.

Subordinate replica

A Directory replica that is automatically placed on a server if the parent Directory partition has a master, read/write, or read-only replica and the child Directory partition does not.

Subordinate replicas cannot be modified.

SUPERVISOR bindery login

An administrative login that is not represented by an NDS object. Even An NDS User object called SUPERVISOR is not the same as the SUPERVISOR bindery login. You can log in as the bindery SUPERVISOR using the LOGIN /B option. The bindery SUPERVISOR is kept with each server, and is not affected by replication of NDS objects.See also “Bindery context.”

Related utilities: LOGIN and ENABLE LOGIN in *Utilities Reference* .

Supervisor right

A file system right that grants all rights to the respective directory and files.

Also, an object right that grants all access privileges to all objects.

Also, a property right that grants all rights to all properties or to selected properties.

See also “Rights.”

Supported gateway

A protocol that is supported by a Messaging Server object.

For example, you may want the users of your NetWare MHS messaging server to be able to communicate with (non-native) users from a SNADS or X.400 messaging environment. You can add the SNADS and X.400 protocols to the messaging server as supported gateways.

Synchronization

Replica synchronization A means of ensuring that replicas of a Directory partition contain the same information as other replicas of that partition. (See “Novell Directory replica.”)

Time synchronization A method of ensuring that all servers in a Directory tree report the same time. (See “Time synchronization.”)

Synthetic time

A type of time stamp used by Novell Directory Services (NDS) to prevent objects from being timestamped incorrectly.

For example, if the time on the server is changed and no longer matches the timestamp of the partition, then a synthetic timestamp is issued to NDS to prevent objects from being timestamped incorrectly.

See also “Time synchronization.”

System (Sy) attribute

A file system attribute that marks directories or files for use only by the operating system.

See also “Attributes.”

SYSTEM directory

The SYS:SYSTEM directory, created during network installation, that contains NetWare operating system files as well as NLM programs and NetWare utilities for managing the network.

By default user ADMIN, or a user with ADMIN equivalent rights, has rights to the SYS:SYSTEM directory.

Don't delete the SYSTEM directory.

See also "File system" ; "LOGIN directory" ; "MAIL directory" ; "PUBLIC directory."

System Fault Tolerance

(SFT) A means of protecting data by providing procedures that allow you to automatically recover from hardware failures.

There are three levels of SFT; each level of redundancy (duplication) decreases the possibility of data loss.

- **SFT Level I: Hot Fix** ensures that data is not saved to faulty blocks on the server's hard disk. (See "Hot Fix.")

- **SFT Level II: Disk Mirroring or Duplexing** protects against hard disk failures by pairing two hard disks on the same channel. The disks operate in tandem, constantly storing and updating the same files. (See "Disk mirroring.")

  Disk duplexing pairs two disks on different channels, which protects data from the failure of the hard disk or the channel that joins the hard disk to the NetWare server. (See "Disk duplexing.")

- **SFT Level III: Server Mirroring** provides protection from server failure with a secondary, identical server that immediately takes over network operations when the primary server fails. (See "Server mirroring.")

Each level of SFT protection includes the previous levels; that is, SFT III includes level I and level II protection.

See also “Data protection.”

System Independent Data Format

(SIDF) The format standard SBACKUP uses. All data backed up using SBACKUP can be read by other backup applications that read and write SIDF.

System login script

In NetWare 3, a type of login script that sets general environments for all users.

In NetWare 4, the container login script replaces the system login script.

See “Container login script” ; “Login scripts.”

System Network Architecture

(SNA) IBM's proprietary networking architecture first introduced in 1974.

SNA is the technology that makes it possible to connect LAN systems to IBM mainframe computers.

SNA has reached a position of prominence in the computer industry based on its completeness and its continued support by IBM.

Chapter 19 *T*

Tape backup device

Either an internal or external tape drive that backs up data from hard disks.

Target

Any server, workstation, or service on the network which has a Target Service Agent loaded. A target can have its data backed up or restored.

If you are backing up and restoring to the host server, the target and the host are the same.

See also “Host” ; “Target Service Agent.”

Target Service Agent

A Target Service Agent (TSA)TSA is a program which runs on a server or workstation that, in conjunction with an SMS compliant backup engine (such as SBACKUP) allows data from a specific workstation or server to be backed up and restored.

When using SBACKUP, the host sends requests to the Target Service Agent, which

- Receives the commands from SBACKUP and processes them so that the target operating system can handle the request for data
- Passes the data request from SBACKUP to the target
- Receives the requested data from the target and returns it to SBACKUP in standard SMS format

Servers and workstations running different software releases, or having different operating systems, require NetWare-compatible Target Service Agents to communicate with SBACKUP.

When a Target Service Agent is used in conjunction with a NetWare Navigator host, the TSA allows the network supervisor to distribute and install business-critical applications, desktop operating systems, and network operating systems to the target server or workstation.

See also “Backup hosts and targets” ; “Storage Management Services.”

Target Service Agent resources

Categories of data, referred to as *major resources* and *minor resources* , created by each Target Service Agent. (See “Major resource” and “Minor resource.”)

Because these resources vary with each Target Service Agent, SBACKUP processes these resources in different ways.

See also “Target Service Agent.”

Task-switching support software

The TBMI2.COM and TASKID.COM files that act as a buffer and manager between IPX and SPX requests and an application's calling process in a task switching environment.

When a task switch is made during an application's call process, the task-switching support software in NetWare ensures that IPX and SPX transport protocols send the call to the proper network resource. This prevents any breaking down of communication between IPX and software processes when a task switch is made.

Use support software if you use a DOS task switcher or if you switch DOS sessions within MS Windows in standard or real mode.

If your application requires the NetWare task-switching support software and you do not use it, your client workstation may experience session failure.

TCP/IP

(Transmission Control Protocol/Internet Protocol) An industry-standard suite of networking protocols that enables dissimilar nodes in a heterogenous environment to communicate with one another.

TCP/IP is built upon four layers that roughly correspond to the seven layer OSI model. The TCP/IP layers are

Process/application
Host to host
Internet
Network access

NetWare TCP/IP

A collection of NLM programs that support applications requiring TCP/IP connectivity. Its routing capabilities forward IP traffic from one network to another.

NetWare TCP/IP uses Routing Information Protocol (RIP) to communicate the internet's configuration with other routers.

It also provides communication between NetWare (IPX) networks across an IP internet that doesn't directly support IPX. This is known as *IPX/IP tunneling.*

NetWare TCP/IP also provides a transport interface for higher-level network services. This interface is used by the Network File System (NFS) and third-party applications written for either the 4.3 BSD UNIX socket interface or the AT&T* Streams Transport Layer Interface (TLI).

NetWare TCP/IP supports Ethernet, token ring, and ARCnet networks through the ODI.

It works with any network adapters of these types supported by a NetWare driver certified for NetWare 3.11 and later versions (including NetWare 4).

Time synchronization

A method of ensuring that all servers in a Directory tree report the same time.

Clocks in computers can deviate slightly, resulting in different times on different servers. Time synchronization corrects these deviations so that all servers in a Directory tree report the same time and provide a *time stamp* to order NDS events.

Whenever an event occurs in the Directory, such as when a password is changed, or an object renamed, NDS requests a *time stamp*.

A time stamp is a unique code that includes the time and identifies this event. The NDS event is assigned a time stamp so that the order in which Directory replicas are updated is correct.

NDS uses time stamps to

- Establish the order of events (such as object creation and Directory partition replication)
- Record real world time values
- Set expiration dates

Time stamps are especially important when Directory partitions are replicated and need to be concurrent with one another.

Replication allows Directory partition updates to originate from many locations. As various users update the Directory replicas of the Directory partition, some updates inevitably pertain to the same data.

For example, a user might delete an object and then recreate it. But without a method of recording the order of these events, the Directory could try to create the object and then delete it.

Time stamps allow the Directory to reproduce the order of events accurately.

Time Servers

When you install NetWare 4 on a server, you are prompted to designate it as a Single Reference, Primary, Reference, or Secondary time server.

Each designation performs a particular time synchronization function:

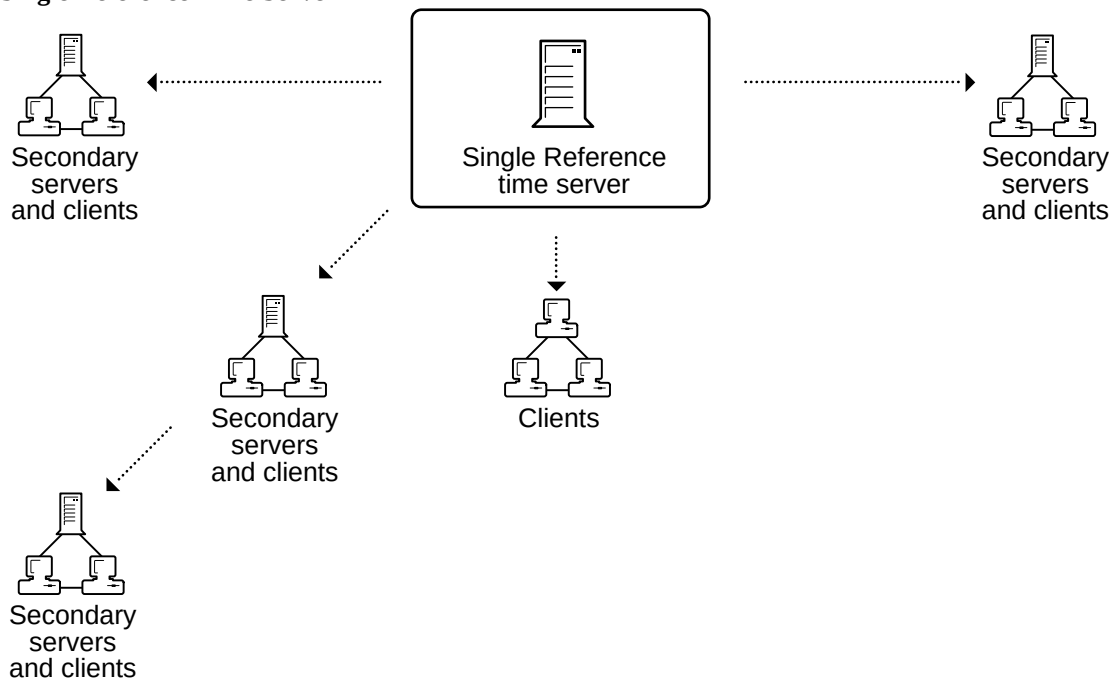
- **Single Reference time server** Provides time to Secondary time servers and to workstations.

This server determines the time for the entire network and is the only source of time on the network. The network supervisor sets the time on the Single Reference time server.

Because the Single Reference time server is the source of time on the network, all other servers must be able to contact it.

The following figure illustrates a Single Reference time server providing time to Secondary time servers and to its own workstations. The Secondary time servers, in turn, provide time to their workstations.

Figure 19-1
Single Reference Time Server



The Single Reference time server works on networks of any size, but this configuration is used primarily for small networks that aren't WANs.

Important

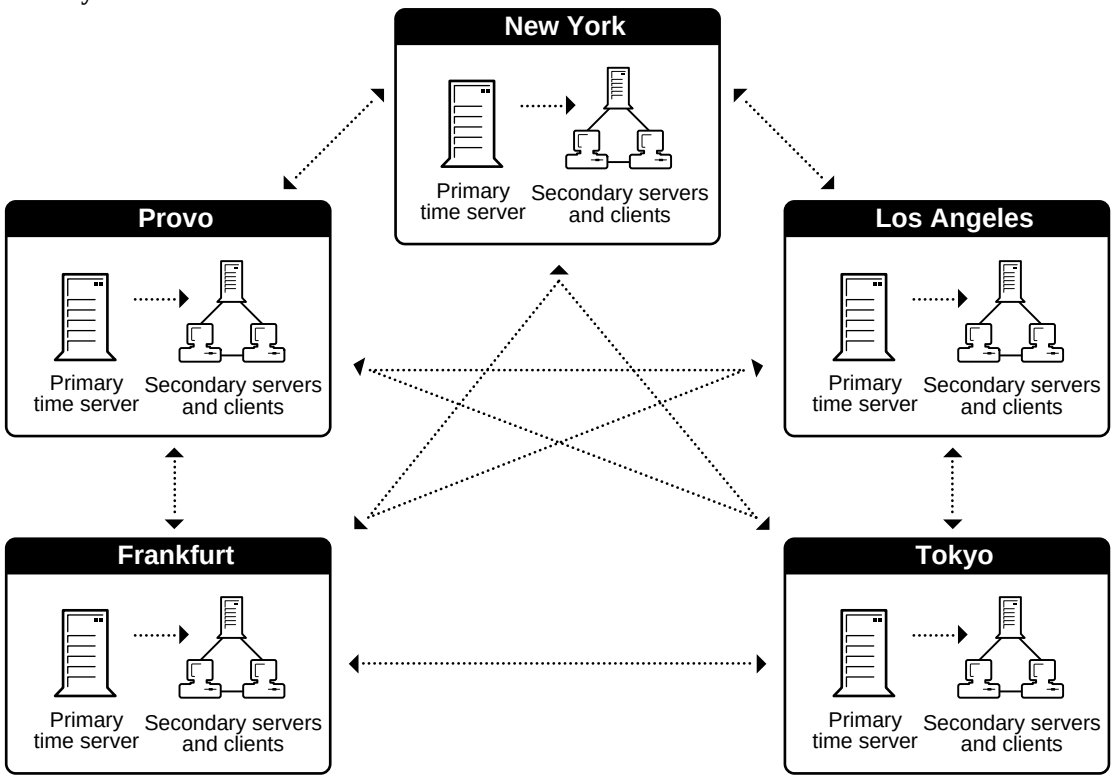
If you use a Single Reference time server, don't use any Primary or Reference time servers on the network.

- **Primary time server** Synchronizes the time with at least one other Primary or Reference time server and provides the time to Secondary time servers and to workstations.

Primary time servers also vote with other Primary or Reference time servers to determine what the common network time should be.

The following figure shows Primary time servers in various locations providing time to their respective Secondary time servers. Secondary time servers, in turn, provide time to their workstations.

Figure 19-2
Primary Time Servers



Use the Primary time server on larger networks to increase fault tolerance by providing redundant paths for Secondary time servers.

If a Primary time server goes down, the Secondary time server can get the time from an alternate Primary time server.

Place a Primary time server in each geographically distinct area so that secondary servers and workstations can access them without using WAN links.

You must have at least one other Primary or Reference time server that the Primary time server can contact. Whenever Primary and Reference

time servers are on a network, they must be able to contact each other for polling.

However, Primary servers do adjust their internal clocks to synchronize with that common network time. Because all Primary servers adjust their clocks, network time may drift slightly.

- **Reference time server** Provides a time to which all other time servers and workstations synchronize.

  Reference time servers may be synchronized with an external time source, such as a radio clock.

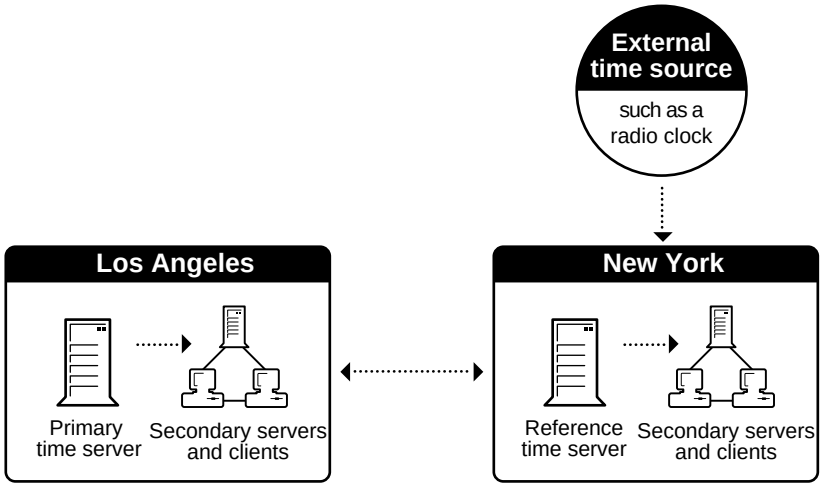
  Reference time servers vote with other Primary or Reference time servers to determine what the common network time should be.

  However, Reference time servers don't adjust their internal clocks; instead, the Primary servers' internal clocks are adjusted to synchronize with the Reference time server.

  Therefore, a Reference time server acts as a central point to set network time. Eventually, all Primary time servers adjust their clocks to agree with a Reference time server.

  The following figure shows a Reference time server synchronized to an external clock. The Reference time server, in turn, provides time to its own secondary servers and workstations, as well as to the Primary time server at another location.

Figure 19-3
Reference Time Server



Use a Reference time server when it is important to have a central point to control time on the network. Usually, only one Reference time server is installed on a network.

You can use more than one Reference time server on a network, but you must synchronize each Reference time server with an external time source, such as a radio clock.

You must have at least one other Primary time server that the Reference time server can contact.

Whenever Primary and Reference time servers are on a network, they must be able to contact each other for polling.

- **Secondary time server** Secondary time servers obtain the time from a Single Reference, Primary, or Reference time server. They adjust their internal clocks to synchronize with the network time, and they provide the time to workstations.

  A Secondary time server doesn't participate in determining the correct network time.

  If you have designated a server on the network as a Single Reference time server, then designate all other servers on the network as Secondary time servers.

If you have designated several servers on the network as Primary or Reference time servers, then designate all other servers on the network as Secondary time servers.

To keep network traffic to a minimum, connect Secondary time servers to Primary or Reference time servers that are physically nearby.

For optimal time synchronization, minimize the number of intervening routers and slow LAN segments between Secondary time servers and their Single Reference, Primary, or Reference time server.

SAP and Custom Configuration

Time source servers use one of two methods to find each other: SAP and custom configuration.

- **SAP** By default, Primary, Reference, and Single Reference servers use SAP to announce their presence on the network.

  Primary and Reference time servers use SAP information to determine the other servers to poll to determine the network time.

  Secondary time servers use SAP information to pick a time server to follow.

  An advantage of SAP is that it allows quick installation without regard to the network layout. It also allows automatic reconfiguration if operating modes are changed or if new servers are added to the network.

  A disadvantage of the SAP method is that it generates a small amount of additional network traffic.

  Another disadvantage is that the SAP method can be disruptive in large network environments where test servers come and go, especially if the test server is polled and its time is substantially different than network time.

- **Custom configuration** You can list the specific time servers that a particular server should contact.

  You can also specify that a server shouldn't listen for SAP information from other time sources and that it shouldn't advertise its presence using SAP.

  An advantage of custom configuration is that the network supervisor maintains complete control of the time synchronization environment.

Also, custom configuration helps eliminate nonessential network SAP traffic, as well as errors associated with accidental reconfiguration.

A disadvantage of custom configuration is the increased time required for planning and installation.

Also, it is more difficult to install or remove Primary, Reference, or Single Reference time servers. You must manually change the approved server list maintained on each server.

Time Synchronization Methods

On small networks where it is unlikely that servers will be added or reconfigured after initial installation, we recommend that you use a Single Reference time server using SAP (the installation defaults).

On larger networks, or on networks subject to frequent *accidental* reconfiguration when servers are added or removed, custom configuration is recommended.

Related utility: TIMESYNC in *Utilities Reference* .

Topology

The physical layout of network components (such as cables, stations, gateways, and hubs). There are three basic topologies:

- *Star network*. Workstations are connected directly to a NetWare server but not to each other.
- *Ring network*. The NetWare server and workstations are cabled in a ring; a workstation's messages may have to pass through several other workstations before reaching the NetWare server.
- *Bus network*. All workstations and the NetWare server are connected to a central cable (a *trunk* or *bus*).

Transaction Tracking System

(TTS) A system that protects data from corruption by backing out incomplete transactions that result from a failure in a network component.

When a transaction is backed out, data is returned to the state it was in before the transaction began.

TTS is a standard feature on NetWare 4 servers.

TTS is extremely important because it protects the Novell Directory database and the queuing database files from corruption.

Warning Do not disable TTS on a server because this prevents updates to the Directory database on that server.

Advantages of Having TTS in the Netware Server

Mainframe, minicomputer, and network database systems have offered transaction backout capability for some time.

However, in most cases this capability is implemented as part of the database application software and not as part of the operating system.

NetWare TTS is implemented at the operating system level on the NetWare server. This method provides two major advantages over application-level implementation:

- **Improved tracking** Transactions are tracked in the NetWare server, where file writes are transacted. Less data is transferred across the network, and all transactions benefit from the speed of the disk caching system in NetWare.

- **Support for applications without backout capability** When a database application without backout capability allocates a physical record lock to a database file or a logical record lock to an open database, the application implies that it is making a transaction.

  At this point, if you have set the correct parameters, TTS begins tracking this implicit transaction so that the transaction can be backed out if a failure occurs.

  When a database application without backout capability releases physical or logical record locks, TTS infers that the application has completed a transaction.

  At this point, TTS ceases tracking the transaction.

  To enable this feature, use the SET command to set TTS parameters.

Three kinds of database applications benefit from TTS:

- Applications that don't have transaction backout capability (implicit transactions)
- Applications that have built-in transaction backout capability (such as Btrieve)
- Applications that use explicit NetWare TTS calls to provide transaction backout capability (such as begin, abort, and end)

TTS Protection

A transaction on a network can be saved improperly in any of the following situations:

- Power to a server or a station is interrupted during a transaction.
- Server or station hardware fails during a transaction (for example, a parity error on a network board).
- A server or a station hangs (a software failure) during a transaction.
- A network transmission component (such as a hub, a repeater, or a cable) fails during a transaction.

TTS protects data from failure in these cases by making a copy of the original data before it is overwritten by new data.

If a failure occurs during the transaction, TTS can back out the transaction and restore the original data.

- If the server fails, TTS backs out the transaction when the server comes up again.
- If a station or network transmission component fails, TTS backs out the transaction immediately.

TTS can protect against these types of failures for any type of application that issues record-locking calls and stores information in records, including traditional databases, some electronic mail applications, and some workgroup appointment schedulers.

Files that aren't organized into discrete records (such as word processing files) aren't protected by TTS.

TTS Operation

TTS guarantees that all changes to a file are either wholly completed or not made at all. To track transactions on a given file with TTS, flag the file as Transactional.

Note A file flagged Transactional can't be deleted or renamed; a file can't be flagged while it is open.

When a workstation begins a transaction in a database file, TTS follows four steps to maintain the integrity of the file:

1. TTS makes a copy of the original data so that the original data can be restored if the transaction fails.

   The copy is placed in a file external to the database file. This external file contains all transaction backout information; only the operating system uses it.

2. TTS writes the changed data to the database file after the copy of the original has been written to the backout file.

3. TTS repeats Steps 1 and 2 for additional changes (a single transaction can consist of a sequence of changes).

4. When all changed data has been written to disk, TTS writes a record to the backout file, indicating that the transaction is complete.

   Completed transactions won't be backed out if the NetWare server, workstation, or network transmission components fail.

Record-Locking Thresholds

Since some database applications leave one or more records locked at all times (usually for copy protection), TTS allows you to set a locking threshold in the workstation.

This locking threshold can be set so that an implicit transaction isn't unnecessarily tracked when the application is started and the first record lock occurs.

Setting the locking threshold prevents having an entire database session tracked as a single transaction or having too many transactions per file update.

Special Backout Cases

In addition to handling routine backout tasks, TTS can back out file truncations or extensions and multiple changes to the same data area during a single transaction.

TTS can also back out interrupted transaction backouts (if the NetWare server fails in the middle of backing out transactions from a previous failure).

TTS also holds all workstation record locks until a transaction is completed. This prevents the disaster that would result from the following situation:

- The application in station 1 releases a lock on a record before the transaction is completed (written to disk).
- Station 2 locks and changes the same record in NetWare server cache memory (also before the first transaction is completed).
- Station 1 fails and station 2 completes its transaction (it is written to disk).
- Because station 1 failed, its transaction is backed out, in this case over the transaction that station 2 completed.

If TTS didn't hold station record locks until transaction completion, the database wouldn't contain the correct information, since the latest transaction (from station 2) would have been incorrectly overwritten with data that existed before the failed transaction (from station 1).

Related utilities: FILER , FLAG , and SET in *Utilities Reference* .

See also “Cache memory.”

Transactional (T) attribute

A file system attribute that indicates the file is protected by TTS.

See also “Attributes.”

Transmission Control Protocol

(TCP) An industry-standard suite of networking protocols that enables dissimilar nodes in a heterogenous environment to communicate with one another.

See “TCP/IP.”

Trustee

A user or group granted rights to work with a directory, file, or object; the object is called a *trustee* of that directory, file, or object.

Rights are granted to objects (making them trustees) by *trustee assignments.* Trustee assignments are part of the directory, file, or object to which they grant access.

Trustee assignments are stored in a *trustee list* . An object's trustee list is stored in the object's ACL property.

For example, to make group WRITERS a trustee of directory PROJECTS, go to PROJECTS and make WRITERS a trustee.

[Public] is a special trustee. You can always specify [Public] as the trustee of a file, directory, or object.

Anyone who tries to access a file, directory, or object without any other rights is allowed the rights granted to the [Public] trustee.

Granting Rights

Trustee assignments for objects and for directories and files are made in the same way, but the rights granted by a trustee assignment are different for objects than for directories and files.

Also, object rights have no affect on directories and files, and file and directory rights have no affect on objects.

One exception exists: A trustee of a Server object with the Supervisor right is automatically granted the Supervisor right to the root directory of each volume on that server.

When you make a trustee assignment to a directory, file, or object, the trustee has access to the directory, its files, and its subdirectories (unless rights are redefined at the file or subdirectory level) or to the subordinate objects. This is called *inheritance* .

Through inheritance, rights granted to a trustee pass down through the structure unless one of the following is true:

- Other trustee assignments are granted for the same object at a lower level of the directory structure
- The Inherited Rights Filter of a subdirectory or file or subordinate object revokes rights granted in a trustee assignment above that point

An explicit trustee of a directory, file, or object is an object that has a trustee assignment to that directory, file, or object.

A *trustee through inheritance* is an object that has a trustee assignment to a directory, file, or object higher in the structure and inherits rights for the current directory, file, or object.

Securing the Directory Tree

A trustee assignment for a file or directory always allows the user to see the path to the root directory of the volume. A trustee assignment for an object, however, doesn't automatically show the user the directory tree to the root.

This security feature, called the *hole in the tree* , prevents a user who has rights in one branch of the tree from jumping over a place where he or she doesn't have rights and then browsing the entire tree.

Similarly, the Supervisor right, which can't be blocked by an Inherited Rights Filter on a file or directory, can be blocked by the Inherited Rights Filter for an object, either for object or property rights.

Important

Use caution when blocking the Supervisor right to objects. If you delete the only object that has the Supervisor right to part of the tree and the Inherited Rights Filter blocks others from inheriting the Supervisor object right, that part of the tree is cut off.

To make trustee assignments for a directory or file, an object must be a trustee of that directory or file with the Access Control right.

To make a trustee assignment for an object, an object must be a trustee of that object with the Write or Add Self right to the object's ACL property.

Related utilities: FILER , NETADMIN , NetWare Administrator , and RIGHTS in *Utilities Reference* .

See also "Inherited Rights Filter" ; "Security."

TSA

A Target Service Agent (TSA) program that runs on a server or workstation and, with an SMS-compliant backup engine (such as SBACKUP), allows data from a specific workstation or server to be backed up and restored.

When using SBACKUP, the host sends requests to the Target Service Agent, which

- Receives the commands from SBACKUP and processes them so that the target operating system can handle the request for data
- Passes the data request from SBACKUP to the target
- Receives the requested data from the target and returns it to SBACKUP in standard SMS format

Servers and workstations running different software releases, or having different operating systems, require NetWare-compatible Target Service Agents to communicate with SBACKUP.

See also "Target Service Agent."

TTS

(Transaction Tracking System) A system that protects database applications from corruption by backing out incomplete transactions that result from a failure in a network component.

See "Transaction Tracking System."

Turbo FAT index

A special FAT index used when a file exceeds 64 blocks (and the corresponding number of FAT entries). NetWare creates a turbo FAT index to group together all FAT entries for that file.

The first entry in a turbo FAT index consists of the first FAT number of the file. The second entry consists of the second FAT number, etc.

A turbo FAT index enables a large file to be accessed quickly.

See also “File Allocation Table.”

Chapter 20 *U*

Unbinding

The process of removing a communication protocol from network boards and LAN drivers.

See “Binding and unbinding.”

UNC redirection

(Universal Naming Convention redirection) A technology that allows you to connect and map to network resources without formally connecting to them.

See “Universal Naming Convention redirection.”

Unicode

A 16-bit character representation, defined by the Unicode Consortium, that supports up to 65,536 unique characters. Unicode allows you to represent the characters for multiple languages using a single Unicode representation.

All objects and their attributes in the Directory database are stored in their Unicode representation.

However, clients (including DOS) use 256-character *code pages* (using 8-bit characters). Not every character created using a given code page displays correctly on a workstation using a different code page. (For more information on code pages, see your DOS manual.)

When you change code pages, you need a different set of Unicode translation tables in order to run NetWare utilities and manage the Directory database.

For example, to use code page 850 (Europe) with country information for France (for which the international telephone country code is 33), you need the following Unicode files:

- 850_UNI.033—translates code page 850 to Unicode
- UNI_850.033—translates Unicode to code page 850
- UNI_MON.033—handles monocasing (the proper alphabetization of upper-and lower-case letters)
- UNI_COL.033—handles collation and sorted lists

For different code pages and locales, you need Unicode tables with corresponding code page numbers and country codes.

If you anticipate managing objects created from different code pages, you must limit object names and properties to characters common to all the applicable code pages.

See also “Code page.”

Uninterruptible power supply

(UPS) A backup power unit that supplies uninterrupted power if a commercial power outage occurs.

Types of UPS are online and offline:

- **Online UPS** Actively modifies the power as it moves through the unit. If a power outage occurs, the unit is already active and continues to provide power.

  An online UPS is usually more expensive than an offline UPS, but provides a nearly constant source of energy during power outages.

- **Offline UPS** Monitors the power line. When power drops, the UPS is activated.

  The drawback to this method is the slight lag before the offline UPS becomes active. However, most offline UPS systems are fast enough to offset this lag.

Because UPS systems can be expensive, most companies attach them only to the most critical devices, such as NetWare servers, routers, and hard disk subsystems.

Attaching a UPS to a server enables the server to properly close files and rewrite the system directory to disk.

Unfortunately, most programs run on the workstation and data stored in RAM is not saved during a power outage unless each station has its own UPS.

If the UPS doesn't have its own form of surge protection, install a surge protector to protect the UPS from power surges.

Universal Naming Convention redirection

(UNC redirection) A technology that allows you to connect and map to network resources without formally connecting to them. Using UNC redirection, you can do the following:

- Use applications and programs within MS Windows to access network volumes and directories
- Assign network applications, volumes, and directories to icons within MS Windows

The following utilities and programs let you set up UNC redirection on your DOS and MS Windows client workstations:

- The MS-DOS NET USE command
- The MS Windows File Manager or Print Manager

NetWare supports the use of UNC redirection for path statements in dialog boxes within the following MS Windows conventions:

- Program group files (.GRP)
- Program items files
- Program information files (PIF)
- Referencing files

UNIX client

A UNIX computer connected to the network.

The UNIX client stores and retrieves data from the NetWare server and runs executable network files. The UNIX client provides multiple NetWare-client multitasking on a single station.

UNIX clients include IPX/SPX and NCP/IPX communication protocols to allow other Novell Clients access to UNIX applications.

See also “Client.”

Unknown object

A leaf object that represents an NDS object that has been corrupted and can't be identified as belonging to any of the other object classes.

After migrating to NetWare 4 from NetWare 3, bindery objects might appear as Unknown objects.

See also “Object.”

Unloading

The process of unlinking NLM programs from the NetWare operating system.

See “Loading and unloading.”

Upgrade

The process of converting your current network operating system to NetWare 4.2 using an applicable Novell upgrade solution. These solutions include:

INSTALL.NLM

This option allows you to maintain the NetWare 4.11 computer as a server by upgrading the operating system to NetWare 4.2.

Across-the-Wire Using the Novell Upgrade Wizard

This option allows you to take NetWare 3.1*x* bindery information and model it to a NetWare 4 Directory tree structure before merging it into the actual NetWare 4.2 Directory tree. Once the bindery is merged into the Directory tree, the NetWare 3.1*x* server files are migrated using the upgrade wizard.

See Installation for information.

Upgrading Non-NetWare Operating Systems to NetWare 4.2

Novell-developed solutions for upgrading from Windows NT* Server, BANYAN* VINES*, LAN Manager*, and LAN Server are available through Novell Consulting Services.

UPS

(Uninterruptible power supply) A backup power unit that supplies uninterrupted power if a commercial power outage occurs.

See “Uninterruptible power supply.”

UPS monitoring

The process a NetWare server uses to ensure that an attached UPS is functioning properly.

A Novell-certified UPS is attached to a server to provide backup power. (You can also attach a UPS to workstations without installing UPS monitoring hardware on the stations.)

When a power failure occurs, NetWare notifies users. After a timeout specified in SERVER.CFG, the server logs out remaining users, closes open files, and shuts itself down.

If you install a Novell-approved UPS, you must also install or set a board in the server to monitor the UPS.

See also “Uninterruptible power supply.”

User Datagram Protocol

(UDP) A transport protocol in the TCP/IP suite of protocols.

UDP is not connection oriented and does not acknowledge data receipt. Because UDP doesn't establish and deestablish connections or control data flow, it performs faster than TCP. However, it is less reliable.

User login script

A type of login script that sets environments specific to a user. Use user login scripts to contain items that can't be included in system or profile login scripts.

User login scripts are optional; if used, they execute after system and profile login scripts.

See also "Login scripts."

User object

A leaf object in NDS that represents a person with access to the network. A User object stores information about the person it represents.

The following items are important to managing User objects:

Login Names

The login name is the name the user logs in with. A login name is mandatory when creating a User object.

You can have a login name of up to 64 characters; however, for efficiency, use one of the following conventions when creating login names:

- Given name (for example, user JANE)
- Surname (for example, user DOE)
- Initials and surname (for example, user JDOE)

Do not use special characters or control characters in a login name. Spaces can be used but aren't recommended.

When you use a login name with spaces in a login script, enclose the entire login name within quotation marks. (To avoid this, use underscores in the login name rather than spaces.)

Group Membership

You can assign a user to Group objects. When added to a group, a user inherits the rights assigned to that group.

Home Directories

A home directory serves as a user's personal workspace.

If you create home directories, plan a parent directory (such as SYS:HOME or SYS:USERS) for them. Or, for a large system, set aside a separate volume for users' home directories.

To simplify system administration, make each user's home directory name the same as that user's login name (for example, SYS:USER\JANE or SYS:HOME\RDSMITH).

If you grant all trustee rights to users in their own directories, users can control access to files in their directories. (Users who have the Supervisor directory right to the directory above home directories still have access.)

This allows users to work on projects in their home directory and prevents others from accessing their work.

Once the work is completed, the files can be copied to a work or project directory (group work space) where other users can access the information.

Trustee Rights

If users need to access specific directories and files (other than those assigned by the system), you must grant users trustee rights to these directories.

Security Equal To Property

The Security Equal To property allows users to exercise rights equivalent to those of another user.

Assigning the Security Equal To property is convenient when you need to give a user access to the same information that another user already has access to.

In networks that contain confidential data for selected users, make sure that you don't inadvertently give a user access to restricted information.

Use particular caution when making a user security equal to a user who has the Supervisor object right.

You can add the Security Equal To property only to User objects. However, every object (including User objects) is automatically security equal to all container objects directly above it. This cannot be altered or modified.

User Login Scripts

These configurable batch files customize the network environment for users by initializing environment variables, mapping drives, and executing other commands.

Up to three login scripts are used at login, executed in the following order:

1. The login script of the user's immediate container
2. The login script in a profile object specified for that user
3. The user's individual login script

Where there are conflicting or contradicting commands in login scripts, the commands in the most recently executed login script are effective.

If no login scripts exist, a default login script executes and maps a drive to NetWare utilities.

Print Job Configurations

Each user can use printing defaults, or you can create print job configurations for a container or User object.

Account Management

Any user who has the Supervisor object right to another User object manages that User object and can modify information about that user.

Users who don't have the Supervisor object right can be granted rights to other User objects to fulfill specific responsibilities. For example, the network supervisor may want only the phone book manager to be granted rights to each user's phone number property.

User Account Restrictions

Every user account can be restricted to prevent unauthorized users from accessing the network. Some restrictions can even disable the account so that no one can log in as that user.

The network supervisor can restrict logins in the following ways:

- **Account balance restrictions** If you install Accounting to monitor or limit network resources, you can assign account balances for users and specify credit limits. When the balance is depleted, the account is disabled.

  If accounting hasn't been installed, this option isn't available.

- **Expiration restrictions** You can specify an expiration date for a user account. For example, set the account to expire at 12:01 a.m. the following day.

  Any attempt to log in after the account expires disables the account. (Default: no expiration.)

- **Password restrictions** You can require passwords.

  If you require passwords, you can also specify the minimum length (default: 5 characters), how often the password must be changed (default: 40 days), whether the user can change the password (default: Yes), and whether the password must be unique (default: No).

  For a password to be unique, it must be different from the previous eight passwords used by the account.

  You can also specify the number of times a user can log in with an expired password (grace logins, default: 6) or the number of incorrect login attempts allowed (default: 6 times).

When either number is exceeded, the account is disabled.

See also “Security.”

- **Disk space restrictions** You can set a limit to the maximum number of blocks available to a user.

- **Connection restrictions** You can limit the number of workstations (connections) from which a user can be logged in at any one time.

- **Time restrictions** You can restrict the hours and days during which users can log in. Times are specified in half-hour blocks. You can assign all users the same times, or you can restrict users individually (default: no time restriction).

- **Network address 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 can log in from.

  Workstation restrictions can't be set with system default restrictions; they must be assigned individually. If no network address restrictions are listed, no station restrictions are in effect.

Related utilities: NETADMIN and NetWare Administrator in *Utilities Reference* .

See also “Accounting” ; “Group object” ; “Login scripts” ; “Security Equal To” ; Creating Leaf Objects , Managing Groups of User Objects , and Cautions When Deleting User Objects in *Supervising the Network* .

User object ADMIN

A User object, created automatically during NetWare 4 installation, that has rights to create and manage objects.

When you first create the Directory tree, ADMIN is given a trustee assignment to the root object. This trustee assignment includes the Supervisor object right, which means that ADMIN has rights to create and manage all objects in the tree.

As you create other User objects in the Directory tree, you can give them the Supervisor object right to create and manage other container objects and all

their leaf objects. Control of the network is as dispersed or centralized as you make it.

After you assign the Supervisor object right to other User objects, you can rename ADMIN or delete it.

However, don't delete ADMIN until you've created other User objects and granted one the Supervisor object right to the root object. Otherwise, no one has full access to the Directory tree.

Unlike SUPERVISOR in earlier versions of NetWare, ADMIN doesn't have any special significance. It is just the first User object created and therefore must have the ability to create other objects.

See also "User object."

User template

Important

This information applies only to the NETADMIN text utility and not to the NetWare Administrator graphical utility. Under NetWare 4.11, NetWare Administrator no longer supports the USER_TEMPLATE object, but instead supports the new Template class of objects. For more information, see Managing User Accounts in the NetWare Administrator online help.

A file containing default information you can apply to new User objects to give them default property values. This helps if you are creating many users who need the same property values.

You create user templates in Organization or Organizational Unit objects.

When you create a User object, you can specify that you want to use a user template. In this case, the property values entered in the user template for that container (or the container above, if no user template exists in the current container) are copied into the new User object as it is created.

The user template saves you from re-entering information—such as a fax number, login time restrictions, addresses, password restrictions, or language—that is common to every User object in a container.

When you create a user template in a container, you can copy information from the parent container's user template.

For example, if you create a template in SALES.NOVELL, you are asked whether you want to start by copying the user template (if one exists) from NOVELL.

A user template is actually a User object named USER_TEMPLATE. You enter information in this object just as you do any other User object, although not all properties of a User object can be copied from a user template.

Information assigned to a new User object from a template can be changed after the User object is created.

However, you can't log in as USER_TEMPLATE, grant rights with a user template, apply a user template to existing User objects, nor apply user template updates to User objects created with that template.

Utilities

Programs that add functionality to the NetWare operating system. NetWare 4 utilities support MS Windows, and DOS environments. (See *Utilities Reference* .)

Server Utilities and NLM Programs

NetWare server utilities and NLM programs run at the server console of a NetWare 4 server.

Use the server utility commands at the server console prompt to

- Change memory allocations
- Monitor how the server is being used
- Control workstations' use of the resources on the server

The server NLM programs link disk drivers, LAN drivers, name space modules, management applications, etc., with the server's operating system.

Workstation Utilities

NetWare workstation utilities can be run from a DOS or MS Windows workstation.

Graphical utilities, new under NetWare 4, allow network supervisors to manage the network through MS Windows.

Text utilities for DOS support both bindery and NDS.

See also “NetWare user tools”; “NetWare Loadable Module.”

Chapter

21 *V*

Value-added process

(VAP) A process that ties enhanced operating system features to a NetWare 2 operating system without interfering with the network's normal operation.

VAPs run on top of the operating system in much the same way a word processing or spreadsheet application runs on top of DOS.

NLM programs provide this type of enhancement for NetWare 3 and NetWare 4. (See "NetWare Loadable Module.")

VAP

A process that ties enhanced operating system features to a NetWare 2 operating system.

See"Value-added process."

VDT

A table that keeps track of volume segment information.

See "Volume Definition Table."

Volume

A physical amount of hard disk storage space, fixed in size. A NetWare volume is the highest level in the NetWare file system (on the same level as a DOS root directory).

In NDS, each volume is also a Volume object in the Directory.

When you create a volume with the INSTALL utility, INSTALL puts a Volume object in the same context as the NetWare server within the Directory tree. By default, INSTALL names the Volume object *servername_volumeobject* .

You can change the context of Volume objects with NETADMIN or NetWare Administrator.

If you rename a volume, change the volume name on the server using the INSTALL utility, and change the volume object's name in the Directory using NETADMIN or NetWare Administrator.

You can create a new volume on any hard disk that has a NetWare 4 partition. A NetWare 4 server supports up to 64 volumes.

NetWare volumes are subdivided in two ways:

- *Logically* . Volumes are divided into directories by network supervisors and users who have the appropriate rights.

- *Physically* . Volumes are divided into volume segments; different segments of a volume can be stored on one or more hard disks.

  A single hard disk can contain up to eight volume segments belonging to one or more volumes, and each volume can consist of up to 32 volume segments.

  By placing segments of the same volume on multiple hard disks, different parts of the same volume can be read from or written to simultaneously, speeding up disk input/output.

  However, when you spread segments of a volume over several disks, protect the volumes against disk failure by mirroring; otherwise, if a single disk fails, one or more entire volumes shut down.

  A volume's size can be increased by adding another hard disk to the NetWare server, by setting up a NetWare partition on the disk, or by adding the new NetWare partition to the existing volume as one or more new volume segments.

  Volume size can be increased, in many cases, while the server is running and the volume still mounted.

The first network volume is named SYS:. Additional volumes can be defined with INSTALL and are assigned volume names between 2 and 15 characters.

Several NetWare utilities—including FILER, MAP, and VOLINFO—list a NetWare server's volume names.

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 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.

When you boot the NetWare server, each volume is mounted, meaning that

- The volume becomes visible to the operating system
- The volume's FAT is loaded into memory

  Each file block of data takes up one entry in the FAT.

  Because of this, volumes with a smaller block size require more server memory to mount and manage.

  However, if most of your files are small, a large block size wastes disk space.
- The volume's DET is loaded into memory

If a volume fails to mount, it might be because you have run out of RAM. This is because the FAT takes up cache buffers.

Related utility: INSTALL in *Utilities Reference* .

See also “File system” ; “Volume Definition Table.”

Volume Definition Table

(VDT) A table that keeps track of volume segment information such as volume name, volume size, and where volume segments are located on various network hard disks.

Each NetWare volume contains a VDT in its NetWare partition.

See also “Volume.”

Volume object

A leaf object that represents a physical volume on the network.

In the Volume object's properties, you can store information about which NetWare server the physical volume is located on and the volume name recorded when the volume was initialized at the server (for example, SYS:).

You can also store information such as the volume's owner, space use restrictions for users, or a description of its use.

You can also view statistical information on disk space availability, block size, directory entries, name space support, etc.

See also “Object” ; “Volume” ; Creating Leaf Objects in *Supervising the Network* .

Volume segments

A physical division of a volume.

Different segments of a volume can be stored on one or more hard disks, allowing you to create large volumes.

A single hard disk can contain up to eight volume segments belonging to one or more volumes, and each volume can span up to 32 segments.

By placing segments of the same volume on multiple hard disks, different parts of the same volume can be read from or written to simultaneously, thus speeding up disk I/O.

You can add segments to a volume (with INSTALL.NLM), but removing a segment from a volume can destroy the volume.

NetWare maintains a VDT that maps the segments on the hard disk to the volume.

See also “Volume.”

Chapter 22 *W*

Wait time

In a NetWare UPS system, the number of seconds the UPS waits before signaling to the NetWare server that the normal power supply is off.

The NetWare server then alerts attached workstations to log out.

See also “Uninterruptible power supply.”

WAN

(Wide area network) A network that communicates over a long distance, such as across a city or around the world.

See “Wide area network.”

Watchdog

Packets used to make sure workstations are still connected to the NetWare server.

All settings are determined by the SET parameters.

You can set parameters so that if the server hasn't received a packet from a station in a certain time, a watchdog packet is sent to the station. If the station doesn't respond within a certain time, another watchdog packet is sent.

If the station still doesn't respond to a certain number of watchdog packets, the server assumes that the station is no longer connected and clears the station's connection.

The time period before the first watchdog packet, the time period between watchdog packets, and the number of watchdog packets is configurable using the SET utility.

Related utility: SET in *Utilities Reference* .

See also “Packet receive buffer.”

Wide area network

(WAN) 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 another local area network.

See also “Local area network.”

Workstation

A personal computer connected to a NetWare network and used to perform tasks through application programs or utilities. Also referred to as a *client* or shortened to *station* .

See also “Client.”

Write right

A file system right that grants the right to open and write to files.

Also, a property right that grants the right to add, change, or remove any values of the property.

See also “Rights.”

Chapter 23 *X*

Xerox Network Systems

(XNS) Novell IPX is a variation on XNS. One major difference between IPX and XNS is that they do not use the same Ethernet encapsulation format. A second difference is that IPX uses Novell's proprietary Service Advertisement Protocol (SAP).

See also "IPX."

XON/XOFF

A handshake protocol that prevents a sending system from transmitting data faster than a receiving system can accept it.

See also "Handshaking" ; "Serial communication."

XNS

(XNS) Novell IPX is a variation on XNS.

See "Utilities."

Chapter 24 *Z*

Zones

Arbitrary groups of nodes on an AppleTalk internetwork. Zones provide divisions in a large internetwork.

Each node belongs to only one zone at a time. The zone that a node belongs to is determined automatically when that node connects to the network.

Zones are referred to by names. Each zone name can be up to 32 characters. (In a network without routers, only one zone exists. The zone name is invisible to users.)

Zone names are converted to addresses on the internetwork by the Name Binding protocol. The names are exchanged by the Zone Information protocol.

Zone names and addresses are maintained in a zone information table within each router. A NetWare server can act as a router for AppleTalk nodes connected to it.