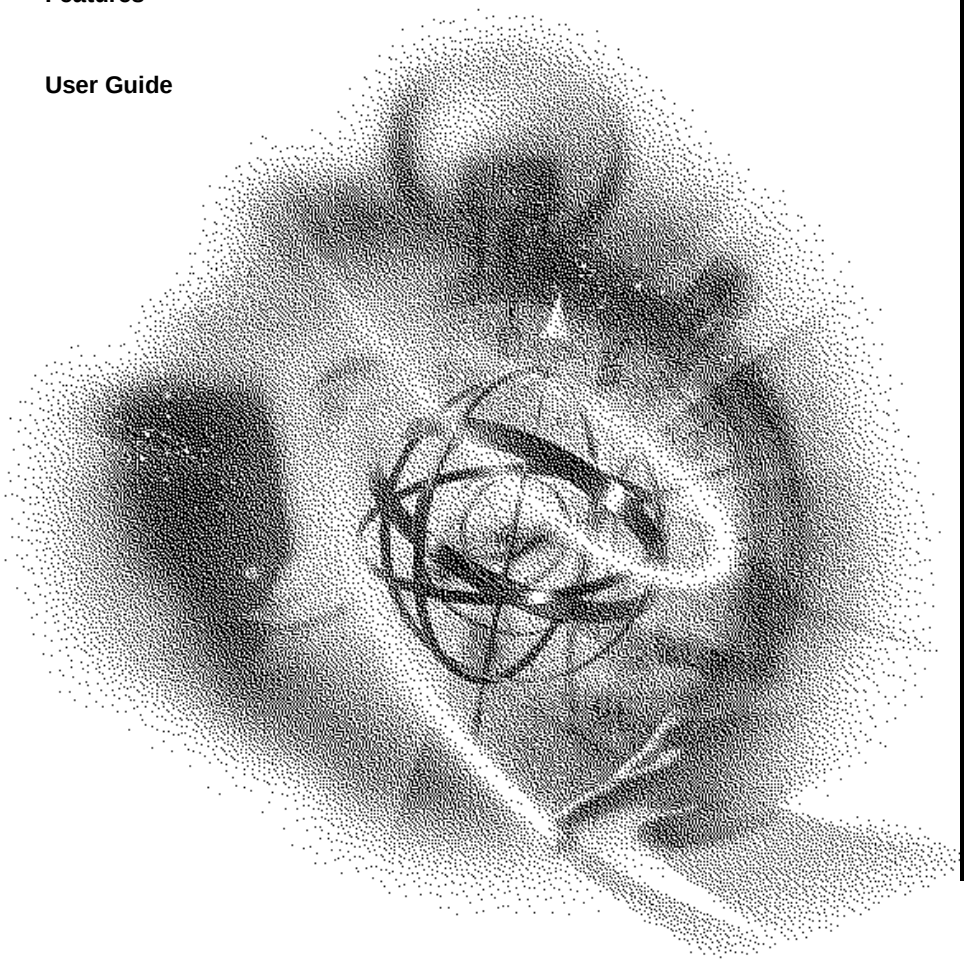
VERSION 4.11

Security

Features

User Guide



NetWare® 4™

Novell®

disclaimer

Novell, Inc. makes no representations or warranties with respect to the contents or use of this manual, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any NetWare software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of NetWare software, at any time, without any obligation to notify any person or entity of such changes.

trademarks

Novell and NetWare are registered trademarks of Novell, Inc. in the United States and other countries. The Novell Network Symbol is a trademark of Novell, Inc.

A complete list of trademarks and their respective owners appears in “Trademarks” on page 45.

U.S. Patent Nos. 5,157,663; 5,349,642; and 5,455,932. U.S. and International Patent Pending.

Novell, Inc.
122 East 1700 South
Provo, UT 84606
U.S.A.

Security Features User Guide
September 1996
100-003612-001 A

How to Use This Manual

1 User Security Responsibilities

2 Logging In

3 Accessing Files and Directories

How to Use This Manual

Introduction

This *Security Features User Guide* describes how users can make effective use of NetWare® Enhanced Security. This guide is designed to

- Help you use the server in a secure manner
- Enable you to use the server's protection mechanisms effectively
- Warn you about possible misuse of mechanisms

For this manual, a *user* is an authorized individual with a network account who interacts directly with the server via a network connection. A user should not have any special privileges to affect the configuration of the system.

By reading this manual, you will learn

- How to log in and log out without compromising security
- Why you may be denied access to certain NetWare Directory Services™ (NDS™) objects
- What server features can maximize the protections offered by the product, and how to take advantage of those features
- How to avoid pitfalls that might compromise the security of the server

If you are a network supervisor, you should also read *NetWare Enhanced Security Administration*.

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 ™.

System Overview

The NetWare operating system is a distributed network operating system made up of three components:

- Servers
- Workstations
- Network media

The evaluated server component described in this manual can serve any number of workstations using the network media, limited only by software license restrictions.

The server component contains a Network Trusted Computing Base (NTCB) partition, which is used to enforce the security policies and to protect data stored on the server.

The evaluated server component *cannot* be used to run untrusted software.

Server Security Mechanisms

This section summarizes the protection mechanisms that are provided by the NetWare Enhanced Security server. Some of these mechanisms occur transparently, while others must be invoked by the user or the network supervisor.

- Trusted systems are trusted to protect information—that is, to allow access to data objects only in accordance with the system's access control policies.

  The server implements separate access control policies for NDS objects, NDS object properties, and file system objects (FSOs). These policies permit access based on a user's "need to know" as defined by authorized administrative or nonadministrative users.

- The access control mechanisms provided by the server component depend upon the principle of individual accountability; that is, the server is able to identity and authenticate each user before allowing access to the server's protected resources and to trace the user's subsequent security-relevant actions.

  Identification and authentication (I&A) requires the user to enter a security token ("This is who I am…") and authentication token ("…and here is some secret information to prove it").

  The server provides traceability by allowing an auditor to audit security-relevant events within the system.

- Finally, the server provides assurances that the security policies are implemented correctly and that the system is "self-protecting."

The following sections summarize the protection mechanisms provided by the NetWare Enhanced Security server component.

Identification and Authentication

A NetWare server allows you to log in from workstations throughout the network. However, the server does authenticate your identity before before allowing you to use server resources.

Authentication is based on your user identifier and your private password. Each user's identifier is unique.

The password is a text string, known only to you. It is associated with your user identifier and recognized by the server NTCB (Network Trusted Computing Base).

NetWare 4.*x* authentication consists of two parts: network login and background authentication.

In a network login, your workstation participates in a protocol with the server to obtain a credential and signature, based on the Rivest, Shamir, Adelman (RSA) private key associated with your user account.

Once the server obtains the credential and signature, the background authentication protocol allows the workstation to present the credential and signature to any server on the network, gaining services from that server.

Thus, it is not necessary to log in separately to each server in the network.

Each user may have as many as three types of associated login restrictions:

- The days of the week and times of day when logins are permitted
- An account balance
- The list of IPX™ (Internetwork Packet Exchange™) addresses that can be used to originate connections

The server provides a flexible intruder detection mechanism to detect and prevent brute-force password-guessing attacks. If the number of incorrect login attempts exceeds the specified parameter, the server locks that station for a configurable period of time (or until the station is enabled by a network supervisor).

The server also provides a NetWare 3.*x* login method that uses the same authentication materials, but uses different protocol messages to transfer the authentication materials to the server. In a NetWare 3.*x* login, the user logs in to a "bindery context" on a single server.

Discretionary Access Control

The server NTCB (Network Trusted Computing Base) partition enforces DAC (discretionary access control) policies for all named objects under its control. These policies are based on user identity, where each user has the same identity on all servers.

The primary named objects controlled by the server's NTCB partition are NDS objects, NDS object properties, and file system objects (FSOs). Each of these objects has a separate access control policy.

An overview of these policies is not presented here. For a description of the access controls on NDS objects and NDS object properties, see:

- *Guide to NetWare 4 Networks*
- Chapter 1, "Managing NetWare Directory Services Objects," of *Supervising the Network*
- *Concepts*
- Chapter 3, "Security Supplement to Installation," and Chapter 5, "Security Supplement to Managing Directories, Files, and Applications," of *NetWare Enhanced Security Administration*

For information on file system access controls, see:

- Chapter 2, "Managing Directories, Files, and Applications," of *Supervising the Network*
- Chapter 6, "Security Supplement to Creating Login Scripts," of *NetWare Enhanced Security Administration*

In addition to the primary named objects, other types of named objects include messages, semaphores, logical record locks, queues, queue entries, currently printing jobs, and audit trails.

Audit Trails

Three types of audit trails are provided in the server component:

- **NDS audit trails** are associated with NDS containers (and therefore are known as "container auditing"), and are replicated along with the containers. The auditor may preselect NDS auditing on a per-event basis.
- **File system audit trails** are associated with volumes within the server. The auditor may preselect file system audits on a per-event, per-user, or per-file basis.
- **Workstation audit trails** are stored and protected on the server.

Object Reuse

The server enforces an object reuse policy to prevent scavenging of information for storage objects. In general, objects are cleared prior to their release to a subject.

As a network system composed of three components—servers, workstations, and network media—NetWare is designed to meet the Controlled Access implementation (Class C2) requirements of the *Trusted Network Interpretation* (*TNI*) [NCSC-TG-005] of the *Trusted Computer System Evaluation Criteria* (*TCSEC*) [DoD5200.28-STD].

The evaluated server is an IAD component as defined in Appendix A of the *Trusted Network Interpretation*.

Manual Overview

The NetWare operating system has been carefully designed, implemented, and administered to operate securely. You must read and follow the instructions in this manual in order to effectively use the NetWare operating system's protection mechanisms.

This manual is organized as follows:

- "How to Use This Manual," which you are currently reading, explains the purpose of this guide and points you to other relevant manuals.
- Chapter 1, "User Security Responsibilities," on page 11 discusses what a NetWare Enhanced Security user is, and hence what security responsibilities such a user would have.
- Chapter 2, "Logging In," on page 17 explains the procedures for logging in to the network from your workstation.
- Chapter 3, "Accessing Files and Directories," on page 21 describes how to manage files and directories on the server. This chapter also describes how access to file system objects can be controlled and how access control information can be manipulated based on the appropriate access rights.

- Chapter 4, “Accessing NDS Objects,” on page 31 describes how to control access to NDS objects in order to safeguard information.
- Chapter 5, “Messaging,” on page 33 describes how you can send messages to other users via the server.
- Chapter 6, “Printing and Queuing,” on page 35 describes operations for print services and queue management.
- Chapter 7, “Logging Out,” on page 39 explains the procedures for securely logging out from the network.

Use of This Manual

This manual describes the security features available to you as a user of NetWare Enhanced Security servers. In order to meet the requirements of the NetWare Enhanced Security environment, you must use only trusted workstations to access NetWare servers. Your network supervisor can tell you how to identify trusted workstations.

This manual describes security aspects of NetWare servers. In addition to this manual, the vendor of your trusted worsktation will provide a companion manual that describes how to use your trusted workstation securely. This manual refers to the companion manual as a “workstation security features user guide”; your network supervisor can tell you the exact title of the workstation manual.

In order to use a NetWare network securely, you must read and understand both this manual and the workstation manual.

Related Manuals

This following related manuals may be useful in conjunction with this manual:

- *Concepts*
- *NetWare Client for DOS and Windows User Guide*
- *Installing and Using Novell Online Documentation*
- *Guide to NetWare 4 Networks*
- *Print Services*
- *Supervising the Network*
- *Utilities Reference*

User Comments

We are continually looking for ways to make our products and our documentation as easy to use as possible.

You can help us by sharing your comments and suggestions about how our documentation could be made more useful to you and about inaccuracies or information gaps it might contain.

Submit your comments by using the User Comments form provided or by writing to us directly at the following address:

Novell, Inc.
Documentation Development MS C-23-1
122 East 1700 South
Provo, UT 84606 USA

We appreciate your comments.

chapter 1

User Security Responsibilities

Within the context of NetWare® Enhanced Security, a *user* is an authorized individual with a network account who interacts directly with a server via a network connection.

As a user, you may have multiple logins if you have multiple roles. Users do not share login identities, but a user may be assigned multiple login names for different roles within the network.

Once logged in, you may access—create, view, modify, or delete—files on any server within the network for which you have the appropriate rights. Other services available to you include

- NetWare Directory Services™ (NDS™)
- Print services
- Audit services
- Interprocess communication services

These services are all subject to some form of access control.

User Responsibilities

You are responsible for network security. This includes such basics as protecting your password, not leaving your client workstation unattended while you are logged in, and adequately protecting hard copy based on its sensitivity.

Passwords

If passwords were not required, nearly anyone with access to a client workstation could access the NetWare server.

Before you can access a NetWare server, your network supervisor must give you a login ID and password. You should then change your password immediately.

Select a new password that is at least eight characters in length. Avoid using passwords that might be guessed, such as the name of your child, your dog, or your favorite football team. If you must use such a password, adding a few symbols can increase its security—for example, #dolphins@.

You should not tell anyone your password or write it down. If you must write the password down, you must be able to somehow protect it on your own.

The server protects your password internally, provided you only type your password at the login prompt. Do not use this same password for screen savers, E-mail programs, or other programs on your client workstation unless doing so is within your client workstation's security guidelines.

Your network supervisor may have specified a password expiration date for your server password. However, you may want to change your password more frequently (at least every three months) and certainly any time you think your password has been compromised.

For more information on changing you password, see "NetWare Password Change" on page 19.

Access Control

You should understand the access control policies in effect before modifying any access rights. Otherwise, you may unintentionally grant or deny access to files or directories.

There are three main access control policies, governing the following three classes of objects:

- NDS objects
- NDS object properties
- File system objects (FSOs)

The two policies for NDS objects are described in Chapter 4, "Accessing NDS Objects," on page 31. The file system object policy for files and directories is described in Chapter 3, "Accessing Files and Directories," on page 21.

The NDS policies provide controls down to individual NDS objects such as NetWare Volume objects. The file system object policy provides more finely grained access control for individual files and directories within a volume.

All users (including network supervisors) are subject to all of the access control policies described in Chapters 3 and 4.

Chapter 3 also covers how to make the deletion of files permanent. (Simply deleting a file does not prevent another user from undeleting the file and reading its contents.)

In addition to the main classes of objects—NDS objects, NDS object properties, and file system objects—you can manipulate two other classes of objects:

- Logical record locks
- Semaphores

NetWare does not include any tools for directly manipulating these objects; they are for use by NetWare-aware applications.

Logical Record Locks

A logical record lock allows you to associate a name with a group of filenames and to lock or unlock the names as a group. The ability to access a logical record lock says nothing about the rights to the underlying filenames; the filenames can be considered arbitrary text strings.

You can lock and unlock logical records created by other users if you know the name of the lock. Administrators can query the list of logical record locks as well as the filenames they refer to.

Creation of a logical record lock implicitly grants access for all other users to lock or unlock the logical record. Logical record locks have no configurable access control; thus, the access rights to a newly created logical record lock allow universal access.

Logical record locks cannot be explicitly deleted. Once created, they continue to exist until they are no longer in use by any connection, at which point they are automatically destroyed. The memory associated with the logical record lock in the server is then available for reallocation.

There is no permanent storage associated with a logical record lock; that is, when a server is booted, there are no logical record locks, and logical record locks do not survive over reboots.

Semaphores

Semaphores are very similar to logical record locks—you can create them, lock them, and unlock them. As with logical record locks, semaphores cannot be explicitly deleted, but rather are automatically deleted when no one is using them or when a server reboots.

When you create a semaphore, you give it a name. Anyone who knows the name can lock and unlock the semaphore. Network supervisors can obtain a list of semaphores. There is no configurable access control for semaphores.

Removable Media

Only you, the user, can safeguard data that you have external to the system (for example, hard copy output).

Similarly, you should not disclose file contents to other users by any means—hard copy output, diskettes, etc.—unless authorized to do so.

Other User Activities

When you load software on your client workstation, you must be careful not to introduce viruses. For the necessary precautions for your client, see your client administrator.

You must not leave your client unattended if you are currently logged in to the server. To do so would allow others to access objects (such as files) that you have access to on both your client and server(s).

You should not rely on screen savers on your client to prevent a sophisticated user from accessing your data, unless your client provides a screen saver that meets your security requirements. If you must use a screen saver, use different passwords for the screen saver and for logging in.

The best way to prevent unauthorized access to an unattended client is to log out when you are finished with your session. For instructions on logging out, see Chapter 7, “Logging Out,” on page 39.

chapter 2

Logging In

Before you can access programs and data on a NetWare® server, you must log in. To do this, you must identify yourself to the system (by entering your login name) and prove that you are who you say you are (by entering your password). If you enter a valid name and password, you will normally be granted access to the network.

Network supervisors may place restrictions on the time of day and the days of the week you can log in, or on what workstations you can use to log in. Check with your network supervisor to determine whether any such restrictions apply.

Logging In to the Server

To make a logical connection on a NetWare network, you must prove that you are an authorized user. This is done when you provide your user identification and a valid password.

NetWare servers provide bindery and NDS™ (NetWare Directory Services™) logins.

- If you use a bindery login, you are proving your identity to a NeWare server and must repeat the identification process each time you want to access resources on another server.

- If you use an NDS login, you prove your identity once. When you want to access another server, software in your workstation proves your identity without your intervention through a process called *background authentication*.

If you use bindery logins, you may have a different identity on each server you communicate with; with NDS, you will have the same identity on each server.

Depending on the type of workstation you have, there may be other limitations. For example, if you are using a DOS- or Windows*-based workstation, you can only be logged in to one NDS identity at a time.

With NDS logins, you need only one server password to gain access to all network resources (such as network directories, printers, and applications) that you have the right to use. For step-by-step instructions for logging in to the network, see your client security features user guide.

If you are using an unevaluated client (rather than a trusted workstation), see your client documentation to determine whether you need to log in using a bindery connection.

The use of unevaluated clients is prohibited in the NetWare Enhanced Security environment.

- If you do *not* need to log in using a bindery connection, see ”Logging In to a NetWare 4 Network” in *NetWare Client for DOS and Windows User Guide*.

- If you *do* need to log in using a bindery connection, see “Logging In to NetWare 4 with a NetWare Bindery Connection” in *NetWare Client for DOS and Windows User Guide*.

If your network contains more than one NetWare Directory tree, you must specify which tree you want to log in to. The specific method used for selecting a tree will depend on you client architecture.

The “Preferred Tree” option in either your VLM.EXE file or your NET.CFG file may work, depending on your client. For instructions, see your client workstation’s security features user guide or trusted facility manual.

VLM.EXE files are described in Chapter 3, “Command Line Parameters Reference,” of *NetWare Client for DOS and Windows Technical Reference*. NET.CFG files are described in Chapter 2, “NET.CFG Options Reference,” of *NetWare Client for DOS and Windows Technical Reference*.

NetWare Password Change

Your password can consist of any sequence of characters from the "character" portion of the keyboard (that is, letters, numbers, and punctuation).

You should not use control characters or function keys as part of your password. Depending on the tool you use, you may be able to set them in your password but subsequently be unable to log in.

The minimum password length is set by your network supervisor. In the evaluated configuration, it is at least eight characters.

Before choosing your password, see "Passwords" on page 12.

You may or may not be able to change your password using the NetWare SETPASS, NETUSER, or NWUSER command.

If you can't change your password, it may be because the network supervisor has configured your account so as to prevent you from changing your password, or because your trusted workstation prevents these utilities from performing password changes. See your client's security features user guide.

For instructions on using these commands, see:

- "SETPASS" in Chapter 2 of *Utilities Reference*
- "NETUSER" ("Change Password" option), in Chapter 2 of *Utilities Reference*
- "Setting a New Password" in Chapter 3 of *NetWare Client for DOS and Windows User Guide* (for the NWUSER command)

Note that passwords set with any of these utilities (SETPASS, NETUSER, and NWUSER) are not case sensitive. The utilities accept both uppercase and lowercase letters so that the passwords "abcdefgh," "AbCdEfGh," and "ABDEFGH" are identical.

However, the utilities supplied with your client may differentiate betweenupper case and lowercase letters. The utilities supplied with your client may also enforce password quality requirements, such as requiring that you have a minimum number of nonalphabetic or nonnumeric characters.

To determine whether your client enforces password quality requirements or differentiates between uppercase and lowercase letters, see your client documentation.

In addition to setting a minimum password length, the administrator may configure your account so that you must have unique passwords. If so, you cannot reuse any of your previous eight passwords (even with a different mixture of uppercase and lowercase characters).

If your password expires, the LOGIN program may prompt you to change your password. If so, change your password promptly.

The LOGIN program may also specify that you have a certain number of grace logins. This is the number of times you can log in with an expired password before your account is disabled.

For instructions on changing an expired NetWare password, see your client's security features user guide.

chapter 3

Accessing Files and Directories

NetWare® Directory Services™ (NDS™) helps you manage network resources such as NetWare servers and printers; however, NDS does not control the file system (directories and files).

This chapter describes the access controls for the file system and utilities to help you manage files and directories.

The file system has three types of structures:

- Volumes
- Directories
- Files

For more information, see "The Structure of the File System" in Chapter 1 of *NetWare Client for DOS and Windows User Guide*.

Also, for information about the file system access and control mechanisms, see "Attributes," "Effective rights," "Inherited Rights Filter," "Rights," and "Security" in *Concepts*.

It is very important that you understand the access control policy in this section before you modify any access rights. Otherwise, you could unintentionally grant or deny access to files or directories.

File System Access Controls

While the NDS access policy only provides controls down to the individual storage volume, the file system access policy provides a more finely grained access control for individual files and directories.

Access to an NDS Volume object is further restricted by the access rights associated with the files and directories stored within the volume. Thus, you may have access to an NDS Volume object but be prohibited from accessing some (or even all) of the files and directories within the volume.

If you have the Supervisor right, you are exempt from all file system access controls on volumes mounted on that server. You have this right if you have either of the following

- Supervisor right to the NDS Server object
- Write right to the NDS Server object's ACL property

These rights are assigned only to network supervisors.

All file system objects have an owner and a trustee list maintained within the file system. Trustee rights determine the access rights that users have to directories and files. For a description of the trustee rights, see "Trustee Rights" in Chapter 2 of *Supervising the Network*.

For information on how assigning directory and file attributes affects other users, see "Directory and File Attributes" in Chapter 2 of *Supervising the Network*.

File System Object Rights

Table 3-1 shows the access rights that are applied to directories and files. If you have either Access Control or Supervisor rights to the file or directory, you can grant access to that file or directory to other users. (The Supervisor right is assigned only to network supervisors.)

Table 3-1
NetWare File System Object Rights

Right	Actions Permitted (Directory)	Actions Permitted (File)
Supervisor	Grants all rights to directory	Grants all rights to file
Read	Open files in directory for read or permit execution	Open file for read, or permit execution
Write	Open files in directory for write	Open file for write
Create	Create new files in directory	Salvage file after deletion
Erase	Delete directory or directory contents	Delete file
Modify	Change attributes of directory or directory contents	Change file attributes/name but not contents
File Scan	View directory name and directory contents	View filename
Access Control	Change trustee assignments and Inherited Rights Filters	Change trustee assignments and Inherited Rights Filters

File system rights can be blocked using Inherited Rights Filters (IRFs). However, unlike NetWare Directory Services IRFs, file system IRFs do not block the Supervisor right.

Some directories on your NetWare server cannot be accessed at any time by any user. There is no way to assign any rights to these directories. Server interfaces that allow setting and retrieving trustee lists do not work with these directories.

File Attributes

Files can have attributes such as Read Only (Ro) and Delete Inhibit (Di). For an explanation of these and other file attributes, see “FLAG” in *Utilities Reference*.

File attributes are not access controls. Setting the Read-Only attribute does *not* ensure that no one can write to the file. Any user with the Modify right to the file can change the Read-Only attribute.

To prevent others from writing to your file, verify that they do not have the Write right to the file.

The Execute Only (X) and Copy Inhibit (Ci) attributes are enforced by clients, not by the server. Do *not* rely on these attributes to protect files.

File Ownership

Every file system object has an owner. The owner is the user who created the object, unless the ownership has been changed by a network supervisor. File ownership is not involved in access control decisions.

Creating Directories

You can create a directory using the FILER text utility. Your client may also supply facilities—such as the DOS MKDIR utility or Windows* graphical utilities—to create directories.

To create a directory, you must have the Create (or Supervisor) right to the new directory’s parent directory.

See “Creating Directories Using FILER” in Chapter 2 of *Supervising the Network*.

Copying or Moving Files

You can copy a file using the FILER text utility. Your client may also supply facilities (such as the DOS COPY utility or Windows graphical utilities) to copy files.

To copy or move files, you must have the File Scan and Read rights (or the Supervisor right) to the source file and the Create (or Supervisor) right to the destination directory.

To move files (that is, to copy them to a destination directory *and* delete them from the source directory), you also need the Erase (or Supervisor) right to the source directory.

See "Copying or Moving Files Using FILER" in Chapter 2 of *Supervising the Network*.

Adding a Trustee

You can add a trustee to a directory or file using the FILER text utility. You must have the Access Control (or Supervisor) right to the file or directory to which you want to add the trustee.

See "Using FILER to Add a Trustee" in Chapter 2 of *Supervising the Network*.

You can also perform this operation using the RIGHTS utility. See "RIGHTS" in *Utilities Reference*.

Deleting a Trustee

You can delete a trustee from a directory or file using the FILER text utility. You must have the Access Control (or Supervisor) right to the file or directory from which you want to remove the trustee.

See "Using FILER to Delete a Trustee" in Chapter 2 of *Supervising the Network*.

You can also perform this operation using the RIGHTS utility. See "RIGHTS" in *Utilities Reference*.

Modifying a Trustee's Rights

You can modify a trustee's rights to a directory or file using the FILER text utility. You must have the Access Control (or Supervisor) right to the file or directory for which you want to change the trustee's rights.

See "Using FILER to Modify a Trustee's Rights" in Chapter 2 of *Supervising the Network*.

You can also perform this operation using the RIGHTS utility. See "RIGHTS" in *Utilities Reference*.

Viewing and Modifying the Inherited Rights Filter

You can view and modify the Inherited Rights Filter (IRF) for a directory or file using the FILER text utility.

You must have the File Scan (or Supervisor) right to the file or directory for which you want to view the IRF.

You must have the Access Control (or Supervisor) right to the file or directory for which you want to modify the IRF.

See "Using FILER to View / Modify the Inherited Rights Filter" in Chapter 2 of *Supervising the Network*.

You can also view the IRF using the RIGHTS utility. See "RIGHTS" in *Utilities Reference*.

Changing Attributes

You can change the attributes of a directory or file using the FILER text utility. Your client may also provide facilities (such as the DOS ATTRIB utility or Windows graphical tools) to change attributes.

You must have the Modify (or Supervisor) right to the file or directory for which you want to change the attributes.

See "Using FILER to Change Attributes" in Chapter 2 of *Supervising the Network*.

Changing the Owner

You can change the owner of a directory or file using the FILER text utility if you have the Supervisor right to the file or directory for which you want to change the owner.

You can also change the owner of a directory or file using the FILER text utility if you have the

- File Scan right to the file or directory
- Write right to the ACL (access control list) for the NDS User object of both the current owner and new owner

See "Using FILER to Change the Owner" in Chapter 2 of *Supervising the Network*.

Viewing a Trustee's Effective Rights

You can view the effective rights a trustee has to a directory or file using the FILER text utility. You must have the Write right to the trustee's ACL to view the trustee's effective rights to a file or directory.

See "Using FILER to View a Trustee's Effective Rights" in Chapter 2 of *Supervising the Network*.

You can also perform this operation using the RIGHTS utility. See "RIGHTS" in *Utilities Reference*.

Viewing Other Information

You can view extended information about a directory or file using the FILER and NDIR text utilities. You must have the Access Control (or Supervisor) right to the directory or file.

For a list of the information you can view, see "Viewing Other Information about a Directory or File" in Chapter 2 of *Supervising the Network*.

See also "Using FILER to View Other Information" and "Using NDIR to View Other Information" in Chapter 2 of *Supervising the Network*.

Salvaging and Purging Deleted Files and Directories

Files deleted from the NetWare server remain on the disk until they are purged. They can be salvaged (undeleted) any time before they are purged. For more information on salvaging and purging files, see "Salvageable files" in *Concepts*.

Purging frees the space used to store the deleted files on the server's hard disk. If a disk runs out of free space, NetWare automatically purges deleted files in order of deletion.

When a file is deleted, any trustee with the Create and Read rights to the file can undelete (salvage) that file if it has not been purged. To make deletion permanent you must do *one* of the following:

- Before deleting the file, make yourself a trustee with the Create right. Then set an IRF to block all rights so that no one else will have the Create right.

Because the Supervisor right cannot be blocked, a user with the Supervisor right can still salvage the file until it has been purged.

- Set the Purge Immediate attribute before deleting. This causes the system to purge the file as soon as it is deleted.
- Use the PURGE command on your client to purge the directory the file is in after the file is deleted.

If the "Immediate Purge of Deleted Files" parameter has been set at the server console, your files will be purged as soon as they are deleted.

Salvaging Deleted Files

Files deleted from the NetWare server can be recovered unless they have been purged.

You can salvage files by using the FILER text utility. You must have the Create right to the file that has been deleted. If the file is in the "Deleted Directories" area, you need the Supervisor right to the file.

See "Using FILER to Salvage Files" in Chapter 2 of *Supervising the Network*.

Purging Deleted Files

Purging files frees disk space on the NetWare server's hard disk. Purged files cannot be salvaged.

You can purge files using the FILER text utility. You must have the Erase right to the deleted file or directory. If the file is in the "Deleted Directories" area, you need the Supervisor right to the file.

See "Using FILER to Purge Files" in Chapter 2 of *Supervising the Network*.

chapter 4

Accessing NDS Objects

This chapter explains how to apply NetWare® Directory Services™ (NDS™) access controls to safeguard your information.

For more information, see Chapter 6, “Creating an Accessibility Plan,” in *Guide to NetWare 4 Networks*. See also “Attributes,” “Effective rights,” “Inherited Rights Filter,” “Rights,” and “Security” in *Concepts*.

NDS Access Control Overview

NetWare Directory Services software helps you manage network resources such as NetWare servers and printers, but it does not provide control over the file system (directories and files).

For a description of the file system access controls and the utilities to help you manage files and directories, see Chapter 3, “Accessing Files and Directories,” on page 21.

For descriptions of access control lists (ACLs), Inherited Rights Filters, effective rights, and security equivalence, see Chapter 6, “Creating an Accessibility Plan,” in *Guide to NetWare 4 Networks*.

NDS objects can be replicated across more than one server—that is, more than one copy of any object may be on the network. Changes made to any copy are replicated to the other copies.

There may be a delay—usually less than a minute—before the change is replicated. If the network fails or a server is unavailable, the delay could be longer.

If you make a change to an NDS object and the change does not appear to be replicating, or if you notice an inconsistency in versions of an object, you should contact your network supervisor to determine the cause.

NDS Access Control Considerations

You must understand the access control policies for NDS objects and object properties before you modify any access rights. Otherwise, you might incorrectly grant or deny access to other users.

You are responsible for safeguarding your information. If you have the right to change an object's attributes, you need to consider who else has the right to read that object's attributes and whether they should have access to the new attribute.

In an extreme case, if you have the server supervisor privilege (the Supervisor right to the NDS Server object or the Write right to the NDS Server object's ACL property) and you grant such access to another user, that user is exempt from all file system access controls.

In general, you will have rights to read most of the attributes of your NDS User object (except certain restricted values, such as your password), and to modify (write) some of the attributes of your NDS User object, including your login script and print job configuration.

Depending on your site's security policy, you may have rights to modify other attributes of your User object, such as your telephone number or mailing address. In addition, you may also have rights to read or write attributes of other NDS objects.

To determine which NDS object attributes you have rights to read or write, check with your network supervisor.

chapter 5

Messaging

Messaging Capabilities

You can broadcast messages to all users connected to a server, or to specified users only. You can specify users by their connection numbers. Individual users can choose to accept or reject messages. By default, users accept messages sent to them.

When you send a message, the recipient also receives your username and connection number. Messages generated by the server (typically to inform you of an error condition) or sent by the supervisor from the server console do not include a username or connection number.

Message Access Control

Sending a message implicitly grants read and destroy access for the message buffer being sent to the designated receiver, and no access to any other user. Thus, no explicit access control is necessary. Messages

- Are automatically destroyed upon reading
- Can only be read by the connection they are sent to
- Can only be deleted by the person they are sent to (or by the server if overwritten by a console or server-generated message)
- Cannot be recovered after they are deleted
- Are automatically destroyed when the recipient logs out

Messages are sent to *connections*, not to users. Thus, the user who receives the message is whatever user happens to be using the connection number to which the message was sent.

Your responsibility is to verify that the connection number corresponds to the person for whom the message is intended. To do this, you should determine the intended recipient of the message by finding his or connection number immediately prior to sending the message, and then recheck the connection number immediately after sending the message to verify that the same user is still using that connection.

If a user already has a message queued that he or she hasn't read, you won't be able to send the user another message until the queued message has been read.

An exception is the network supervisor at the server console; a message sent from the console overwrites and destroys any queued message from another user.

To minimize the risk of losing messages, you should read messages as soon as you're notified that they're pending.

The NetWare® SEND command can be used at a DOS workstation to send a message to one or more users. SEND allows you to reject all messages (using the /A=N option) or to reject all messages except those coming from the console (using the /A=C option). SEND also allows you to display messages only when polled (using the /A=P option).

The NetWare server implements the option to accept or reject all messages; the other options are implemented by the NetWare client software running in the workstation.

Only users that are logged in can send and receive messages. In addition, if a message is queued for a live connection and the message is not read before the connection is terminated, the message is destroyed as part of the connection termination.

For information on sending a message to a user or a group of users on the network, see "NetWare Send Message" in Chapter 3 of *NetWare Client for DOS and Windows User Guide*.

For information on sending a message to a user or a group of users on the network with NETUSER, see "Using NetWare User Tools for DOS (NETUSER)" in Chapter 3 of *NetWare Client for DOS and Windows User Guide*.

chapter 6

Printing and Queuing

Print security on a network requires careful handling of print files, because data is not sent directly to a printer as it is when printing from a single computer. Instead, the data is stored in a print queue while waiting to go to a printer.

This chapter deals with security considerations related to printing on a NetWare® network and describes print utilities that help you control the print process.

Only you can protect hard copy output. If your installation uses unattended printers (no operator to remove printouts from the printer and hand them to the right user) and you are concerned about others reading your printout, retrieve your print job as soon as you send it.

NetWare User Tools

Printing tasks include

- Setting printer options
- Connecting and disconnecting print queues
- Making print queue connections permanent

CAPTURE

Normally, the CAPTURE utility redirects output from your client to a network printer or file. If you are not logged in, CAPTURE attempts to log you in as user GUEST with no password.

However, the GUEST account does not exist in the NetWare Enhanced Security configuration. In the NetWare Enhanced Security configuration, CAPTURE prompts you for your login name and password.

To determine whether it is acceptable to provide your username and password to the CAPTURE utility, see your client workstation's security features user guide.

For more information, see "Using CAPTURE" in *Print Services*.

NPRINT

NPRINT is used to print files from outside of your application. For more information, see "Using NPRINT" in *Print Services*.

PSC

The PSC utility allows you to perform tasks at the command line that you might otherwise perform using PCONSOLE. PSC monitors and controls printer and print server status from the command line and provides a layout of your printing setup.

For more information, see "Using PSC" in *Print Services*.

PCONSOLE

PCONSOLE creates, assigns, modifies, deletes, and monitors print queues, print servers, and printers. PCONSOLE can also send, monitor, modify, pause, resume, and delete print jobs.

You can use PCONSOLE to view or modify the print status of your current job only. You cannot see or modify the status of other users' jobs.

For more information, see “Viewing or Modifying a Printer’s Status” in *Print Services*.

NETUSER

NETUSER is a client utility used to perform a variety of network tasks. NETUSER printing tasks include

- Capturing output from your client to a network printer
- Printing files from outside of an application
- Monitoring print queues

NETUSER can also be used to send, redirect, monitor, modify, or delete print jobs.

For more information, see “Printing Tasks Handled Through NETUSER” in *Print Services*.

PRINTCON

PRINTCON creates, modifies, and deletes print job configurations that are used to simplify use of the CAPTURE, NPRINT, and PCONSOLE utilities.

For more information, see “Printing Tasks Handled through PRINTCON“ and “Working with Print Job Configurations” in *Print Services*.

PRINTDEF

PRINTDEF defines printer forms for use in CAPTURE, NPRINT, and print job configurations. It also defines print devices in a database for use in print job configurations.

For more information, see “Working with Printer Forms” and “Working with Print Device Definitions” in *Print Services*.

chapter 7

Logging Out

You should log out from the NetWare® server whenever you leave your workstation unless you can safeguard your workstation while it is unattended. Safeguards might include

- A facility provided by the workstation
- Locking the door to your office

The server logout program affects your connections to NetWare servers. Logging out from the server does not necessarily affect the session on your client, except that references to the server's network drives—other than to the LOGIN directory—are no longer valid.

If you log out without specifying a NetWare server name in the LOGOUT command, your client's resource connections to all servers on the network are terminated.

However, you can log out from one server and remain attached to other servers by specifying the server name in the LOGOUT command.

Logging Out from All Servers

To log out from all servers, type:

LOGOUT <Enter>

The system displays a message similar to the following:

```
User USERNAME has been logged out from server
SERVERNAME connection 15.
Login time:         1-06-96     8:01:23 am
Logout time:        1-06-96     5:04:17 pm
User USERNAME has been logged out of Directory
Services tree CORPORATE.
```

In this case, the user is logged out from all NDS™ servers and from the NetWare Directory tree.

Logging Out from a Particular Server

To log out from a particular server, type:

LOGOUT *servername* <Enter>

In this case, the user is logged out from only a single server and is still authenticated to the NetWare Directory tree.

For more information, see your client's security features user guide. See also "Logging Out of a NetWare Server or Network" in Chapter 8 of *NetWare Client for DOS and Windows User Guide* (which covers logging out in DOS as well as from Windows*).

chapter 8

NetWare Programming

This section describes the client-server architecture and provides programming instructions for workstation developers in the NetWare® Enhanced Security environment.

For client workstations to communicate on a network, they must use the same protocol being used on the network.

Client-Server Architecture

A client-server network has at least one computer configured as a NetWare server.

The server is a computer running the NetWare network operating system. The server controls communication and shared network resources.

The client workstations are the individual computers connected to the network.

Protocols

The protocols used for manipulating shared resources include

- NetWare Core Protocol™ (NCP™)
- Storage Management Services™ Protocol (SMSP)
- Print Server Status and Control Protocol (PSSCP)
- Printer Communications Protocol (PCP)

NetWare Core Protocol

NetWare Core Protocol (NCP) handles every service a client 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
- Printing

NetWare Core Protocol consists of approximately 500 NCP interfaces.

These interfaces are identified by number (for example, 0x2222 22 15) and a descriptive name (for example, Rename Directory).

NCP is layered directly on top of IPX™.

Storage Management Services Protocol

The Storage Management Services Protocol consists of approximately 35 interfaces used by clients for backing up and restoring data on servers.

These interfaces are identified by a number (for example, 0x0020) and a descriptive name (for example, SMSP_GetTargetServiceAddress).

SMSP is layered on top of SPX™, which is layered on top of IPX.

Print Server Status and Control Protocol

The Print Server Status and Control Protocol consists of approximately 30 interfaces used by administrators for configuring print servers and by users for inquiring about the status of a print server.

These interfaces are identified by number (for example, 0x0E) and a descriptive name (for example, AbortPrintJob). PSSCP is layered on top of SPX, which is layered on top of IPX.

Printer Communications Protocol

The Printer Communications Protocol consists of approximately 10 interfaces used by print drivers (in either a client or a server) for sending data from print servers to printers. These interfaces are identified by a number (for example, 7) and a descriptive name (for example, Reclaim).

PCP is layered on top of SPX, which is layered on top of IPX.

Trademarks

Novell Trademarks

Internetwork Packet Exchange and IPX are trademarks of Novell, Inc.

NetWare is a registered trademark of Novell, Inc. in the United States and other countries.

NetWare Core Protocol and NCP are trademarks of Novell, Inc.

NetWare Directory Services and NDS are trademarks of Novell, Inc.

NetWare Loadable Module and NLM are trademarks of Novell, Inc.

Novell is a registered trademark of Novell, Inc. in the United States and other countries.

Open Data-Link Interface and ODI are trademarks of Novell, Inc.

Third-Party Trademarks

MS-DOS is a registered trademark of Microsoft Corporation.

Windows is a registered trademark of Microsoft Corporation.

User Comments

We want to hear your comments and suggestions about this manual. Please send them to the following address:

Novell, Inc.
Documentation Development
MS C-23-1
122 East 1700 South
Provo, UT 84606
U.S.A.

Fax: (801) 861-3002

NetWare 4.11
Security Features User Guide
Part #100-003612-001 A
September 1996

For technical support issues, contact your local dealer.

Your name and title: _____

Company: _____

Address: _____

_____

_____

Phone number: _____ Fax: _____

I use this manual as ❑ an overview ❑ a tutorial ❑ a reference ❑ a guide ❑ _____

	Excellent	Good	Fair	Poor
Completeness	❑	❑	❑	❑
Readability (style)	❑	❑	❑	❑
Organization/Format	❑	❑	❑	❑
Accuracy	❑	❑	❑	❑
Examples	❑	❑	❑	❑
Illustrations	❑	❑	❑	❑
Usefulness	❑	❑	❑	❑

Please explain any of your ratings: _____

_____

_____

_____

_____

In what ways can this manual be improved? _____

_____

_____

_____

_____

You may photocopy this comment page as needed so that others can also send in comments.