

PLAN 4000™

File Server User's Manual

NESTAR

NESTAR SYSTEMS, INCORPORATED

PLAN 4000 (TM)

FILE SERVER
USER'S MANUAL

DISCLAIMER OF WARRANTIES

The information in this document has been carefully reviewed and is believed to be reliable; nevertheless, Nestar Systems, Incorporated makes no warranties, either express or implied, with respect to this manual or with respect to the software described in this manual, its quality, performance, merchantability, or fitness for any particular purpose. The entire risk as to its quality and performance is with the buyer. The software herein is transferred "AS IS".

Nestar Systems, Incorporated, reserves the right to make changes to any products described herein to improve their functioning or design. Nestar programs are licensed products whose use is defined in the Nestar System Software License Agreement. Server Programs require a separate license for each machine on which they run.

In no event will Nestar Systems, Incorporated be liable for direct, indirect, incidental, or consequential damages at law or in equity resulting from any defect in the software, even if Nestar Systems, Incorporated has been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of implied warranties or liability for incidental or consequential damages, so the above limitation or exclusion may not apply to you.

The Regents of the University of California, Apple Computer, Inc., and International Business Machines, Inc. make no warranties, either express or implied, regarding the computer software programs described herein, their merchantability or their fitness for any particular purpose. UCSD, UCSD Pascal, and UCSD p-System are all trademarks of The Regents of the University of California. CP/M is a registered trademark of Digital Research, Inc. Z-80 is a registered trademark of Zilog, Inc. Softcard is a trademark of Microsoft Consumer Products.

This document is copyrighted and all rights are reserved. This document may not, in whole or part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent, in writing, from Nestar Systems, Incorporated.

Copyright 1981, 1982, 1983 by Nestar Systems, Inc.
2585 E. Bayshore, Palo Alto, California, 94303
(415) 493-2223 Telex 171420 Nestar PLA

Publication number SC40-0200-0
All rights reserved.

How To Use This Manual

This manual is designed to provide a description of the PLAN 4000 File Server. When familiarizing yourself with your network, read first the General Information Manual, which provides an overview of the PLAN 4000 system.

Read this manual for a discussion of file servers, which allow you to share hard disk storage with other network users. Your particular workstation computer and operating system environment are discussed in the appropriate User's Guide. A bibliography of PLAN 4000 system manuals and guides will be found at the end of this manual.

The material in this document applies to Version 2.0 of the File Server software.

We welcome your criticisms and suggestions. Forms for reporting program errors, and documentation errors or inadequacies are provided at the back of this manual.

Contents

Disclaimer	ii
How to Use This Manual.....	iii
Contents.....	v
Chapter 1 General Information	
1.0 Network Operation.....	1-1
1.1 File Server Commands.....	1-2
Chapter 2 Disk Organization and Pathnaming Conventions	
2.0 Introduction.....	2-1
2.1 Disk Units.....	2-2
2.2 Files.....	2-2
2.3 Directories.....	2-3
2.4 Virtual Volumes.....	2-4
2.5 Pathnaming Conventions.....	2-4
2.6 Default Directory.....	2-9
2.7 Passwords.....	2-10
Chapter 3 Protection	
3.0 Introduction.....	3-1
3.1 Virtual Volume Protection.....	3-2
3.2 User Classes.....	3-3
3.3 Passwords and Access Rights.....	3-5
3.4 Default Access Rights.....	3-7
3.5 The PROTECT command.....	3-8
3.6 The SHOW PROTECTION Command.....	3-8
3.7 Preset Passwords.....	3-9
3.8 Access Rights Needed for Network Commands.....	3-10
3.9 What Happens If You Forget a Password...	3-12

CONTENTS

3.10 Usage Modes and the MOUNT Command..... 3-12

Chapter 4 Locks

4.0 Locks..... 4-1

4.1 LOCK Command..... 4-1

4.2 UNLOCK Command..... 4-2

4.3 SHOW LOCK(S) Command..... 4-3

Chapter 5 File Server Commands

File Server Commands..... 5-1

CREATE..... 5-6

DELETE..... 5-14

HELP..... 5-16

LIST..... 5-18

LOCK..... 5-22

MOUNT..... 5-25

PATHNAME..... 5-28

PROTECT..... 5-30

PROTECTION..... 5-33

RENAME..... 5-34

SET DIR..... 5-36

SET password..... 5-38

SHOW DATE..... 5-40

SHOW DIR..... 5-41

SHOW ID..... 5-42

SHOW INFO..... 5-43

SHOW LOCK..... 5-46

SHOW [ALL] LOCKS..... 5-47

SHOW [ALL] MOUNTS..... 5-49

SHOW PROTECTION..... 5-52

SHOW STATION..... 5-54

SHOW TIME..... 5-55

SHOW TYPE..... 5-56

SHOW TYPES..... 5-58

SHOW VOLS..... 5-59

TIMESTAMP..... 5-60

UNLOCK..... 5-61

UNMOUNT..... 5-62

CONTENTS

Appendix

A Error and Information Messages..... A-1

Index

Bibliography

Reader Comment Form

Chapter One

Introduction to the System

1.0 Network Operation

The PLAN 4000 System links personal computer workstations. You can use your workstation as a standalone computer with local disk drives and printers, while sharing hard disks and printers with others on your network. You can communicate with stations on your network and other networks, local and remote.

The PLAN 4000 network supports a variety of personal computers and operating system environments. General information about sharing hard disks is contained in this manual; information specific to a given microcomputer and operating system is found in the separate user guides listed in the bibliography at the end of this manual.

Two kinds of stations comprise the PLAN 4000 network: user and server. User stations run programs, communicating over the network with each other and with servers. Server stations perform one or more specific tasks for workstations, allowing them to share peripherals on the network. This manual discusses the servers, called "file servers", that control your network's shared hard disks.

The network divides those shared disks into "nested directories" and "virtual volumes" (or "virtual diskettes"). Virtual volumes are formatted to resemble real diskettes. You can use these volumes (portions of a shared hard disk) just as if they were real diskettes inserted in a real local disk drive.

INTRODUCTION

File servers control the hard disks. While microcomputer workstations can be programmed to perform file server tasks, the PLAN 4000 file servers are special devices built specially to perform as network servers. You communicate with the file servers by issuing file server commands from your workstation, via a program called NET. These commands allow you to

- create virtual volumes on shared hard disks
- access these volumes by "mounting" them on "virtual drives" (just as real diskettes are inserted into real drives at your workstation).
- otherwise share and manipulate hard disk space.

Certain virtual volumes on network hard disks are shared by all users with the same type of workstation and operating system. These shared volumes contain libraries of useful utility and system programs, and may be "mounted" automatically for you when you start up.

1.1 File Server Commands

File server commands are discussed in Chapter 5. Additional information on these commands is available in the user guide for your workstation environment. In general, these commands are issued by using a NET program at your workstation. This program allows you to issue commands that will create virtual volumes on your network's hard disks, protect them with passwords, and use them as you would real diskettes. File server commands can also be issued from within programs that you write

yourself.

Before describing these commands, this manual discusses the names given to virtual volumes on the hard disks (Chapter 2), using passwords with these volumes (Chapter 3), and cooperative sharing of network resources (Chapter 4).

Chapter 2

Disk Organization and Pathnaming Conventions

2.0 Introduction

Before you begin using file server commands at your workstation to access the shared hard disks on your network, you will need to learn the file naming conventions that apply to the disks. You will be using portions of the hard disks that have been formatted to resemble real diskettes, and that exist as files on the hard disks. These files are referred to as "virtual volumes" or "virtual diskettes". To create and use them, you must learn how to name them.

SOMETHING TO REMEMBER: virtual volumes, which are files on a hard disk, have a network file name or volume name, to be used when accessing the volume. In some environments, they also have an internal volume name, to be used in your workstation operating system environment. These two names are not the same. You will learn to use the network file name, called a pathname, when using file server commands to create or access a volume, and to use the internal volume name, when it exists, in your local operating system environment.

This is an important point. Since you will probably be issuing both file server and operating system commands from your local environment, you will need to decide which name or command is appropriate: file server pathname and command to manipulate a virtual volume (a hard disk file), or operating system volume name and command to manipulate files within the volume.

PATHNAMES

2.1 Disk Units

Your file server manages the disk space on one to four hard disk drives. Refer to each disk by its assigned name or drive number (disk drives may or may not be given names when they are formatted at your workstation). Hard disks are numbered 1 through 4, and may have names (chosen by your system manager), such as MAIN or ALT, as will be shown below. Such a disk is referenced in file server commands by typing

/MAIN or /2

as the first part of a volume or directory name (pathname).

The file server itself boots from one of these hard disks. You can use the "null" disk name / to refer to the root directory of the disk that the file server boots from (usually /1).

2.2 Files

The file structure on each physical disk unit has two distinct levels:

1. the network level, a hierarchical collection of directories and files formatted as virtual diskettes.
2. the operating system level, where program, text, and data files are stored within a single virtual diskette.

The network level files on each disk unit consist of:

one root directory

and optionally

subdirectories

virtual diskettes

system binary utility programs and data files

In this manual, the expressions "file server virtual volume", "virtual volume", and "virtual diskette" will be used interchangeably. The word "file" will be reserved for the program and data files contained within a single virtual volume and controlled by the workstation operating system. The expression "file server" is used to refer to the special network station that processes file server commands and transfers files to and from shared disks.

2.3 Directories

The root directory on a given physical disk unit points, either directly or through subdirectories, to every virtual volume on that unit. It cannot point to virtual volumes on other physical units.

Each root directory and subdirectory consists of names and disk addresses of subdirectories and virtual diskettes on the same physical unit as the directory itself. A directory that contains the name and address of a given virtual volume will be referred to as the parent directory of that virtual volume.

Directories are automatically expanded as necessary.

For example, a hard disk containing 20 volumes of data and 20 volumes of text might have one

PATHNAMES

main or root directory and two subdirectories:

/MAIN

/MAIN/DATA

/MAIN/TEXT

In /MAIN/DATA will be listed the 20 data volumes, which will have network file names (pathnames) such as /MAIN/DATA/19 (pathnames are explained below). /MAIN/TEXT will contain a listing of the 20 text volumes.

2.4 Virtual Volumes

Virtual volumes are of many types. They can vary in size, as specified by their creator. Chapter 5 discusses their creation. The user guide for your operating system provides additional information on the creation and use of virtual volumes.

The network also uses Text volumes. Text volumes are used by various network programs and contain, for example, electronic mail. Text volumes do not contain a user station operating system directory (catalog).

2.5 Pathnaming Conventions

To address a virtual volume on the PLAN 4000 system, it is necessary to specify its "pathname" by some combination of defaults and explicit names. These consist of:

the physical disk unit (i.e its root directory), either by name or by number

intermediate subdirectories (if any)

the name of the virtual volume.

To address the root directory itself, only the physical disk unit number or name needs to be specified.

Here are a few examples of how pathnames are used with the LIST and CREATE file server commands (discussed in Chapter 5 in detail):

2.5.1 Pathname: /unitnumber

LIST /4

This command lists all the subdirectories and virtual volumes whose names and addresses are included in the root directory on hard disk unit 4. The initial slash indicates that the first field is the name or number of a physical disk unit.

2.5.2 Pathname: /unitname

LIST /MAIN

This command lists all the virtual volumes whose names and addresses are included in the root directory of the system hard disk called MAIN (regardless of which physical disk unit it is located on).

LIST /

Here, the contents are listed of the root directory from which the file server has booted.

All units should have unique names. If, however, your installation has two hard disks with the

PATHNAMES

same name (such as /MAIN), the command LIST /MAIN will display the contents of the disk with the higher unit number. If /1 and /2 are both /MAIN, for example, LIST /MAIN is the same as LIST /2.

2.5.3 Pathname: /unitname/subdirectory

LIST /LANGUAGES/FRENCH

This command causes a search for the physical disk unit named LANGUAGES and for its root directory, which contains the name and address of the subdirectory FRENCH. FRENCH is then read and the virtual volumes in it are displayed.

2.5.4 Pathname: /unitname/subdirectory1 /subdirectory2/virtual volume

CREATE /MAIN/USERS/JANE.DIR/JANE.V1,T=P

This command:

searches for the physical disk unit MAIN

looks in its root directory for the subdirectory USERS

looks in USERS for JANE.DIR

allocates space on the physical disk unit MAIN for the virtual diskette JANE.V1 formatting it to resemble an Apple // UCSD Pascal diskette.

enters the name and address of JANE.V1 in the subdirectory JANE.DIR.

If the subdirectories USERS and JANE.DIR in the

above example do not exist, the CREATE command creates them as needed.

2.5.5 Pathnames: Formal Definition

In general terms, a pathname is specified according to the following definitions. Square brackets indicate optional parameters, e.g. [:password].

pathname: /unitname/filepath
or filepath

unitname: 1, 2, 3, or 4 [:password]
or name [:password]
or //

filepath: name [:password] [//filepath]

name: the name of a disk unit (root directory), subdirectory, virtual disk or network utility. A name has the following restrictions:

1-15 characters.

No commas, slashes, colons, carriage returns, ASCII control characters, or unprintable characters.

Acceptable characters: 0-9, A-Z, !, ", #, \$, %, &, ^, (,), *, <, >, ?, [,], {, }, ~, ~, @, _ , |

Upper and lower case letters are not distinguished (ABC=abc=Abc=)

PATHNAMES

Imbedded blanks are okay. Leading and trailing blanks are removed automatically.

The first character can be any acceptable character.

password: a word used to restrict access to a directory or virtual file. Same restrictions as name, except that control characters may be used in order to permit non-printing for visual security.

(Programmers will notice that this is a "recursive" definition in that a form for filepath includes a filepath. Another way to describe a legal filepath is to say that it consists of one or more names separated by slashes, and each name may be followed by a colon and a password. Recursive definitions will be used elsewhere in the manual to concisely describe sequences of terms.)

Four other rules apply to the pathname:

1. The total pathname cannot exceed 80 characters (including /'s).
2. Upper or lowercase can be used for any characters within a file server command, and are equivalent.
3. An initial slash indicates the pathname begins in the root directory of a physical disk unit. If there is no initial slash, the current default directory is prefixed to the pathname.
4. Blanks before and after the slashes in a pathname are optional and are ignored. Blanks

within file or directory name are part of the name.

Control characters are permitted in file server passwords. If the passwords are set or provided by programs running on the network, no difficulty is encountered. However, the presence of serial cards in user and server stations will prevent the console use of some control characters, since these characters have meanings assigned to them by the serial cards.

For example, attempting to type in a password with a particular control character embedded in it might cause the entire console line to be removed.

The following 16 control characters should NOT be used in file server passwords:

A C E F H I J M N R S T V W X Z

Those recommended for use are the following 10:

B D G K L O P Q U Y

2.6 Default Directory

In order to reduce the number of characters to be typed and processed, the user may specify a default directory. Whenever a pathname is specified that does not begin with a slash, it is prefixed by the current default directory. In the previous example, assume that the subdirectories USERS and JANE.DIR exist before the CREATE command is issued. If so, Jane will achieve the same result if she enters:

```
SET DIR /MAIN/USERS/JANE.DIR
CREATE JANE.V1,T=P
```

PATHNAMES

The SET DIR command above sets the current default directory to:

```
/MAIN/USERS/JANE.DIR
```

which is prefixed to the JANE.V1 when the CREATE command is executed. Thus the create command above is equivalent to:

```
CREATE /MAIN/USERS/JANE.DIR/JANE.V1,T=P
```

The SHOW DIR, LIST, PROTECT, and SHOW PROTECTION commands can be specified with no pathname; if so, each operates on the current default directory. A SET DIR with no pathname clears the current default directory. The SHOW DIR command displays the name of the current default directory.

2.7 Passwords

As will be explained more fully in Chapter 3 (Protection), it is possible when creating a subdirectory or virtual volume to require that a password be specified each time the subdirectory or virtual volume is accessed for some or all operations. In our last example, let's suppose the passwords needed are:

```
x (for the root directory MAIN)
y (for the subdirectory USERS)
z (for the subdirectory JANE)
```

If her current default directory is set for some other directory, Jane would enter:

```
CREATE /MAIN:x/USERS:y/JANE:z/4,T=P
```

or alternatively:

```
SET DIR /MAIN:x/USERS:y/JANE:z  
CREATE 4,T=P
```

It is also possible to set a password for the disk 4, and to set default passwords so that they do not have to be entered each time the pathname is specified; these options are explained in Chapter 3.

Chapter 3

Protection

3.0 Introduction

The PLAN 4000 File Server allows many users to share a large database. However, universal access is not always desirable: files must not be accessed at sensitive times or by unauthorized users. The file server fully controls user station access to the shared database and manipulation of the data.

The file server has three software mechanisms for protecting stored files.

1. Virtual volume protection, a system of passwords and access rights for different classes of users
2. Usage modes, a means of temporarily reserving file system resources for exclusive or restricted use.
3. Locks, which allow users to synchronize access to any resource; for example, external devices or individual files on a virtual diskette (discussed in Chapter 4).

These three mechanisms differ in the following ways:

Passwords and access rights control the usage of virtual diskettes and directories. The protection is involuntary: passwords and access rights allow only the usage that was specified for the virtual diskettes and directories when the protection was set.

PROTECTION

Usage modes allow the user to temporarily restrict access to given virtual diskettes and directories (that is, to restrict access while the disks and directories are mounted). Volumes can be mounted for:

- a. exclusive read/write (EXC)
- b. exclusive write and shared read (UPD)
- c. shared read/write (SHR)

Locks can be used to control access to any resource - e.g., a printer, plotter, scientific instrument, or individual file on a virtual diskette. Locks are voluntary; they provide a convention that cooperating stations can use. The system returns the information that a lock is in use or in exclusive use, but it does not prevent the user from addressing the printer, the particular file, or whatever he or another user is trying to protect.

3.1 Virtual Volume Protection

Each virtual volume can have three different classes of users who have different passwords and are allowed to do different things. When a virtual volume is created, the password required and the access rights allowed for each class of user are specified. This section describes:

the user classes and access rights

how to assign passwords and access rights with the CREATE and PROTECT commands

what the default access rights are for each class of user

preset passwords

access rights needed to execute various file server commands

3.2 User Classes

Potential users of a given virtual volume are divided into three classes:

- public (PUB) users who do not specify a password
- group (GRP) users who specify the group password
- private (PRV) users who specify the private password

The access rights which may be granted or denied to each class of user are:

- R the ability to read the data part of the virtual volume
- W the ability to write on the virtual volume
- E the ability to erase (remove completely) the virtual volume
- C the ability to create a new entry in the directory (meaningful only for directories)
- D the ability to delete an entry from the directory (meaningful only for directories)

A file server volume is removed from the system by the DELETE command. Accomplishing this requires two operations: the volume itself is removed (erased), and the entry in the directory which pointed to the volume is removed (deleted). The E (erase) access right is

PROTECTION

required to erase the volume; the D (delete) access right is required in the corresponding directory to delete the directory entry.

For example, suppose a given PLAN 4000 system at an installation wants to have accounting programs on a Pascal volume called ACCOUNTING. They want ACCOUNTING to be listed in a directory called ADMINISTRATION, which in turn will be listed in the root directory of the system hard disk called /MAIN.

They want to limit access to the directory and volume as follows:

1. public: the public will have no access rights.

2. group a select group of employees will be able to:

R read the virtual diskette and execute the programs on it.

The group password will be SILVER.

3. private The person in charge of the programs will be allowed to:

R read the virtual diskette

W write on the virtual diskette

E erase (remove completely) the virtual diskette

He or she will also be allowed to:

D delete entries from the directory

C create new entries in the directory

The private password will be SAFE.

The access and usage rights for this example are established in the following section.

3.3 Passwords and Access Rights

Passwords and access rights can be specified for a new file server file by a CREATE command and for an existing file server file by a PROTECT command. With [optional] parameters indicated by square brackets, the syntax of these two commands (typed on one line):

```
CREATE pathname,type[,size][,protection][,drive]
      [,usage]
```

```
PROTECT pathname [,protection]
```

For a complete discussion of CREATE and PROTECT see the individual command descriptions in Chapter 5. For an explanation of the [,usage] option, when CREATE is used to mount a new disk, see 3.10.

The optional protection parameter is the same for both.

```
protection: protect item [,protection]
```

```
protect items:
```

```
GRPPW=password          (group password)
```

```
PRVPW=password          (private password)
```

```
PUBACC=access rights    (public access rights)
```

```
GRPACC=access rights    (group access rights)
```

PROTECTION

PRVACC=access rights (private access rights)

access rights: a subset (in any order) of the letters RWECD (read, write, erase, create, and delete, as described under "private" in above example)

To specify no access rights, the equal sign is immediately followed by the delimiter: a comma, blank or carriage return. For example:

```
PUBACC=,GRPACC=
```

the CREATE command would be (typed on one line):

```
CREATE /MAIN/ADMINISTRATION/ACCOUNTING,T=P,  
PRVPW=SAFE,PRVACC=RWE,GRPPW=SECURE,  
GRPACC=R,PUBACC=
```

This command creates an Apple // Pascal volume named ACCOUNTING which is listed in the subdirectory ADMINISTRATION which in turn is listed in the root directory of the hard disk. Users giving the password SAFE can read, write or erase ACCOUNTING, but users giving the password SECURE can only read it. Users who do not give the password SAFE or SECURE have no access rights. Users give the password in the form ACCOUNTING:SAFE or ACCOUNTING:SECURE when specifying the pathname in their file server commands. Users must give the password ADMINISTRATION:SECURE or ADMINISTRATION:SAFE when specifying the directory. (Pathnames are discussed in detail in Chapter 2.)

The CREATE command shown above also implicitly creates the directory ADMINISTRATION (assuming it does not already exist). Passwords and

access rights for ADMINISTRATION are the same as for ACCOUNTING, except that create and delete access rights are automatically added to the private rights for the directory. Note that passwords must be given, when set, for each directory and file in the pathname.

For instance, the volume in this example could be mounted for writing by (typed on one line):

```
MOUNT /MAIN/ADMINISTRATION:SAFE/ACCOUNTING:SAFE,
      RW,D9
```

3.4 Default Access Rights

If public, group, or private access rights are not specified in a CREATE command, the PLAN 4000 system sets standard default values:

PUBACC=R (read)

GRPACC=R (read)

PRVACC varies: For a virtual diskette: RWE
(read, write, erase)

For an explicitly created directory: RWECD
(read, write, erase the directory, create and delete entries in the directory)

For an implicitly created directory: the private access rights for the FS file being explicitly created plus CD - create and delete.

Therefore, in the previous example, the field defining private access rights is not necessary because they are the same as the defaults.

WARNING: If a virtual volume has no private

PROTECTION

password, then all of its private access rights are granted to any user, whether he gives no password or some extraneous password. This means that if a virtual volume is created with group password and access rights only, public users will have, by default, private access rights: read, write, and erase. In other words, for group passwords and access rights to have meaning, private passwords and access rights must also be set.

When a virtual volume is created, all directories specified in the pathname which do not already exist are also created; these implicitly created directories are given CD (create and delete) private access rights plus the access rights specified for the virtual volume being explicitly created; they are also given the same private passwords.

3.5 The PROTECT Command

Usually access rights and passwords are set when a virtual volume or directory is first CREATED. The PROTECT command allows the user to modify the access rights and passwords previously set. The syntax is given in Chapter 5. Protect items which are not specified by the PROTECT command are not changed. Anyone giving the private password for the specified virtual volume can issue a PROTECT command; access rights do not apply. If there is no private password then anyone can issue the PROTECT command.

3.6 The SHOW PROTECTION Command

The SHOW PROTECTION command displays the private, group and public access rights currently assigned to the specified file server

volume. Passwords are never displayed, but their existence is indicated by ,PW. The access rights for the current default directory may be displayed by entering SHOW PROTECTION with no pathname.

3.7 Preset Passwords

The SET command allows a user to preset the group and private passwords to be used in subsequent access commands, so that it is not necessary to enter them each time a pathname is specified:

```
SET GRPPW=x
SET PRVPW=y
or
SET GRPPW=x,PRVPW=y   where x and y are
                        passwords
```

This command makes it less likely that an unauthorized person will learn a password and will also cut down on the amount of typing to be done when entering a pathname.

If passwords are in a program, others can read the listing and know what they are. For example, if a password is NO and your program contains the two file server commands:

```
MOUNT /MAIN/GRADES:NO,D9
MOUNT /MAIN/ANSWERS:NO,D10
```

an enterprising student can read your program and learn the password.

Instead, the following Applesoft BASIC program segment shows how passwords can be used in a program without appearing in the listing:

PROTECTION

```
PRINT "ENTER PASSWORD";
INPUT PW$
PRINT CHR$(14);"SET PRVPW=";PW$
PRINT CHR$(14);"MOUNT /MAIN/GRADES,D9"
PRINT CHR$(14);"MOUNT /MAIN/ANSWERS,D10"
```

3.8 Access Rights Needed for Network Commands

In order to execute a file server command with a pathname parameter, a user must have the READ access right for every directory in the pathname (Except for CREATE, where the lowest directory may have only CREATE access). He needs additional access rights for the following commands:

<u>Command</u>	<u>Access Rights Required</u>
CREATE	C (create) for parent directory
DELETE	E (erase) for virtual volume directory being erased D (delete) for parent directory
RENAME	C (create) and D (delete) for parent directory
PROTECT	Must have private password for virtual volume. Access rights irrelevant.
MOUNT	R (read) for directories and other virtual volumes in pathname W (write) for virtual volume file to be mounted, if RW specified.

BRUN

BLOAD R (read) for virtual volumes addressed
by pathname

LIST

SHOW PROTECTION

SHOW DIR

SHOW TYPE

BSAVE W (write) for virtual diskettes
addressed by pathname

Virtual volumes can be created in a directory (added to that directory) if you have C(reate) access rights, even if you don't have R(ead) or W(rite) access rights. You will not be able to MOUNT such files, however, so you should use the form of the CREATE command that creates and mounts the file in one operation if you intend to write into it. Once the file is unmounted, you no longer have access to it. You cannot LIST a directory to which you don't have R(ead) access.

Note that the DELETE command requires two different access rights for two different objects: E (erase) rights for the object to be removed, and D (delete) rights for the parent directory of that object. As an example, suppose that the directory FOO lists three virtual volumes: A, B, and C. To DELETE A, B, or C, the user must have not only the right to erase (remove completely) A, B, or C, but also the right to delete A, B, C from the directory FOO. DELETE, then, erases (removes completely) a virtual volume, directory, and deletes the directory entry that pointed to it. To DELETE (remove) the directory FOO, the user would need erase rights for FOO and delete rights for its parent directory.

PROTECTION

3.9 What Happens If You Forget a Password...

Passwords are actually stored in an encrypted form from which it is impossible to reconstruct the original name. If a password is lost, there is no way to discover it evening by dumping the disk. The only recourse is to have the System Manager use superuser rights to remove or change the password.

3.10 Usage Modes and the MOUNT Command

In addition to the restricted rights which are controlled by the protection attributes of a file server volume access rights may be (voluntarily) limited even further when the virtual volume is actually used. The MOUNT command (or the CREATE command, for newly created volumes) allows a user to mount a specified virtual volume with either READ/ONLY or READ/WRITE access, provided that these are access rights his password entitles him to. For example, if a user gives the private password and has full access rights, he may want to mount his virtual volume with read only rights so as to prevent accidental writes. Usage is an optional parameter for the MOUNT and CREATE commands:

[,usage]

where usage can be RO (READ/ONLY) or RW (READ/WRITE) and SHR (SHaRed), EXC (EXclusive), or UPD (UPDate).

UPD is an Exclusive-Write/Shared-Read mode. Thus, only one UPD mount of a file (either RW or RO) is allowed at a time, but other users may mount the same file RO, SHR.

PROTECTION

If incomplete access rights are given when mounting a volume, the following defaults are used:

Usage Specified	Default Applied
RO	SHR
RW	UPD
SHR	RO
UPD	RW
EXC	RO
none	RO, SHR

Chapter 4

Locks

4.0 Locks

LOCK commands allow several programs to cooperate in sharing a resource on the PLAN 4000 system, such as a particular volume, printer, or other external device. For example, locks can prevent a printer from printing out two volumes simultaneously.

4.1 LOCK Command

To avoid errors, programs that are accessing the same file or device can issue a lock command:

```
LOCK lockname [,usage]
```

where lockname is any name 1-15 characters in length (except ALL) which has been chosen to represent the resource being shared. Usage is either:

SHR shared - more than one user can have the lock set at a given time

or

EXC exclusive - only one user can have the lock set at a given time.

The default for usage is EXC.

LOCKS

The system then returns one of the following messages:

0,OK

41,IN USE

42,IN EXC USE

(or some syntax error messages)

The IN USE message is returned if the lock command specifies EXC (exclusive) usage when another user has already set the specified lock. The IN EXC USE message is returned if the lock command specifies SHR (shared) usage when another user has set the specified lock for exclusive use.

If the program receives the 0,OK message it can proceed to use the printer or update the file or whatever, but if it receives a 41,IN USE or 42,IN EXC USE message it should either go into a wait loop or go on to some other task before reissuing the LOCK command.

4.2 UNLOCK Command

To release a lock, one of the following commands is issued:

UNLOCK lockname

-releases lockname for use by LOCK commands
from other stations

or

UNLOCK ALL

-releases all locks held by this station

The locks held by a station are automatically unlocked when the station is booted. In particular, turning the station off and on or issuing the OFF command will release all locks.

4.3 SHOW LOCK(S) Command

A user can display locks in several ways:

SHOW LOCKS

- displays all locks currently set at his own user station

SHOW LOCK lockname

- displays the station numbers of all user stations currently using the specified lock

SHOW ALL LOCKS

- displays all locks currently being used, and by which stations

Chapter 5

File Server Commands

File server commands are issued by the user, from his or her workstation. These commands are transmitted to a file server that controls one or more shared hard disks.

Use file server commands to create virtual volumes, for network use (that is, allocating shared disk space for your use). Use the commands to set up passwords on your volumes and to display current information about the network.

File server commands consist of a command word followed by a variable number of parameters, some required and others optional. A pathname or subcommand word, if present, must immediately follow the command word; other parameters may occur in any order. The delimiter following a command word must be a blank and the delimiter following a pathname must be a comma; elsewhere, a comma is used as delimiter.

A file server command has the following form (typed on a single line):

```
<0-n blanks><command word><1-n blanks>
<subcommand word><1-n blanks><pathname>
<,other fields>
```

A pathname may have embedded blanks, so a comma must be used to delimit it from the following fields. No blanks may be imbedded in a

```
command word
subcommand word
other fields.
```

SERVER COMMANDS

See Chapter 2 for a full description of pathnames.

A field may have one of three forms:

Keyword (e.g. REPLACE or ALL)

Keyword=Value (e.g. T=D)

Letter value (e.g. D9 for drive 9)

Optional parameters are indicated by square brackets, e.g. [,optional]. The system assigns default values, where meaningful, when optional parameters are not specified; these are given in the descriptions of the individual commands.

Alphabetic characters in a file server commands can be upper or lower case; both cases have the same meaning. For some operating systems this is not important, but for workstations with terminals that display upper and lower case, and from some operating systems, it is convenient. In some environments, file server commands must be preceded by special characters, such as "@". The user guide for your microcomputer/operating system will provide details.

Some of the parameters are explained more fully elsewhere in this manual:

pathnames	Chapter 2
protection	Chapter 3
size and drive	User Guides
number	User Guides

File server commands can be divided into six classes:

SERVER COMMANDS

1. Commands concerned with creating, deleting, naming and protecting virtual file server files (virtual volumes):

CREATE	RENAME
DELETE	SET GRPPW
LIST	SET PRVPW
PROTECT	SHOW PROTECTION

(In some environments; CREATE exists as a separate program. See your Operating System User Guide).

2. Commands concerned with mounting virtual diskettes at a user station:

- a. For all operating systems

```
MOUNT
UNMOUNT
SHOW MOUNTS
```

- b. For local commands, executed by NET or user program

```
SET <slot>
SET <drive>,<drive-status>
SET <drive>,<slot>
SET FS
SHOW DRIVES
SHOW FS
```

The actual syntax depends upon the specific environment. (See the relevant operating system User Guide).

3. Commands concerned with binary virtual volumes (discussed in the user guides for selected environments)

SERVER COMMANDS

BLOAD
BRUN
BSAVE

4. Commands concerned with locks

LOCK
UNLOCK
SHOW LOCK lockname
SHOW LOCKS

5. Commands that set default values (all environments)

SET DIR

6. Commands that give information at the terminal (all environments)

HELP?	SHOW DATE
SHOW DIR	SHOW INFO
SHOW STATION	SHOW TYPE(S)
SHOW VOLS	TIMESTAMP

The remainder of this chapter consists of descriptions of each file server command. The commands are presented in alphabetical order, and each new command or group of commands starts on a new page. For each command, the following information is presented:

the command syntax

an abbreviated statement of what the command does

parameters and defaults

error and information messages

access rights required to execute the command

discussion

examples

All error and information messages are listed in Appendix A. Individual command descriptions include only those messages that are specific to the given command.

CREATE

```
CREATE pathname,type[,size][,sectors]
      [,protection][,drive][,usage]
```

-creates (and mounts, if a drive parameter is given) a new file with specified type, size, drive, passwords, access rights, and usage rights

In environments, a separate program is used to create virtual volumes.

Parameters and defaults:

pathname: For summary, see PATHNAME filed alphabetically with commands in this chapter. For discussion, see Chapter 2.

type:

T=B (binary)	T=P (Apple // PASCAL)
T=C (Apple // CP/M)	T=S (system)
T=D (Apple // DOS)	T=T (Text)
T=I (IBM PC DOS)	T=Y (directory)
T=3 (Apple /// SOS)	T=U (IBM PC p-SYSTEM PASCAL)

[,size]

SIZE=number [.size-unit]

Size of the file to be created may be given in units of bytes, sectors (256 bytes each), blocks (512 bytes each), or K (1024 bytes each). The default unit for size is blocks. The size parameter has the form: SIZE=number[.unit]. Unit may be 'C' for bytes, 'S' for sectors, 'B' for blocks, or 'K' for 1024 bytes. The '.' is optional except where it is needed to resolve

CREATE

ambiguity in the specification of hexadecimal numbers. It is suggested that the '.' be used for readability.

CREATE allows variable sized files to be created within constraints imposed by the environment in which they will be used. The following table shows the algorithm used to determine the size of a file being created given the SIZE= and T= parameters specified.

<u>T=</u>	<u>SIZE=</u>	<u>default</u>	<u>limits on SIZE=</u>
Y	allowed	3.S	0 < SIZE < 32767.S
3	allowed	560.S	0 < SIZE < 65535.S
B	required	-	0 < SIZE < 193.S
C	allowed	560.S	0 < SIZE < 32767.S
P	allowed	560.S	0 < SIZE < 65535.S
D	allowed	560.S	0 < SIZE < 1600.S*
I	allowed	1280.S	0 < SIZE < 65535.S
U	allowed	1280.S	0 < SIZE < 65535.S
T	required	-	1 < SIZE < 32767.S

* VDOS volumes can be created up to 32766.S in size. However, Network Apple // DOS supports only $\leq 1600.S$, extending the VTOC (i.e., DOS managed space) to maximum of 1600 sectors.

CREATE

<u>T=</u>	<u>Resulting Size</u>
Y	SIZE
B	SIZE
P,C,3 I,U,T	SIZE rounded up to multiple of 2 sectors
D	SIZE rounded up to an integral number of tracks

Note that the actual disk allocation may be slightly higher than the sizes listed in the table. For virtual disk type volumes, one extra sector is added by the file server for file descriptor information.

For directories (T=Y), each sector is big enough for ten names, so the default size of three sectors will hold thirty names. Directories will be automatically expanded when required, so that it is usually not necessary to initially allocate directories more than three sectors.

[,protection] See Chapter 3.

protection: protect item [,protection]
protect item:

,GRPPW=password
,PRVPW=password
,PUBACC=access rights (Default: R)
,GRPACC=accgss rights (Default: PUBACC)
,PRVACC=access rights (Default: RWE, virtual
diskette; RWECD, explicitly created
directory; private access rights of
created FS file, plus CD, implicity
created directory)

access rights: set of letters from RWECD (read, write, erase, create, and delete)

[drive]

Dd, where d=number

[,usage]

Specify Type of Access:

RO (read only)

RW (read/write—must have write access)

Default: RO (RW for UPD)

Specify User Class:

EXC (exclusive)

SHR (shared)

UPD (RW usage for only one user at a time;

other users may mount the volume RO,SHR)

Default: SHR, if RO or no usage parameter given
UPD, if RW

Directories (T=Y) and system files (T=S)
may be mounted for read only (RO) access.

See also MOUNT command.

Error Messages

- 13,ILLEGAL NUMBER (NEGATIVE OR TOO BIG)
- 20,TYPE PARAMETER REQUIRED, (T=)
- 21,SIZE OUT OF RANGE
- 23,SIZE PARAMETER REQUIRED WITH T=B
- 24,SIZE OUT OF RANGE (<1C OR >48K)

CREATE

Access Rights Required to Execute a CREATE

- C (create) for parent directory
- R (read) for each directory on pathname except the parent directory

File server file names can be created in (added to) a directory if you have C(reate) access rights, even if you don't have R(ead) or W(rite) access rights. You will not be able to MOUNT such files, however, so you should use the form of the CREATE command which creates and mounts the file in one operation if you intend to write into it. Once the file is unmounted, you no longer have access to it.

Discussion:

The CREATE command:

1. allocates space for specified virtual disk or directory on specified (or default) physical disk unit
2. creates intermediate directories as necessary
3. enters the volume's name in directory preceding it in pathname, or, if not specified, in current default directory
4. stores passwords and access rights on virtual disk or directory being created; these are stored in a special section not accessible to the ordinary user
5. optionally mounts the newly created disk for subsequent I/O

For directories implicitly created because they do not already exist, users are given CREATE and

CREATE

DELETE access rights plus the access rights and passwords specified for the file being explicitly created.

Virtual disks are stamped with time and date upon creation. The SHOW INFO command is used to display this information.

Examples

1. CREATE /1/USERS/NICK/NICK.V1,T=D,
PRVPW=GOODSTUFF,GRPACC=,PUBACC=

This example creates a virtual disk called NICK.V1 on disk unit 1. It also enters the name and address of NICK.V1 in the subdirectory NICK. All three directories and the virtual disk are on disk unit 1.

The created virtual disk is of type DOS. Its size is automatically 16 sectors of 256 bytes, the size of a real minidisk in DOS 3.3.

Anyone who enters the correct pathname and the password GOODSTUFF will be allowed to read, write or erase the virtual disk NICK.V1. Private access rights were not specified, so the defaults for a virtual disk (RWE) are in effect.

Users who do not know the private password are not allowed any access to NICK.V1.

2. CREATE /LANGUAGES/FRENCH/LESSON.3,T=P,SIZE=60

This example creates a virtual disk of type Pascal whose size is sixty 512-byte blocks. The virtual disk is called LESSON.3 and is listed in a subdirectory called FRENCH which in turn is

CREATE

listed in the root directory of a system hard disk called LANGUAGES.

Everyone has full access rights to this virtual disk without giving any password: they can read it and write on it, and if they have create, read, and delete rights for the subdirectory FRENCH, they can delete it.

3. CREATE BRIDGE,T=B,SIZE=10.S,D9,RW,SHR

This example creates a virtual disk called BRIDGE that is of type binary with a size of ten 256-byte sectors. Space is allocated on the physical unit specified in the current default directory, and the name and address of BRIDGE is entered in the current default directory. All users have full access rights. The disk is then mounted on virtual drive 9 for read/write access and shared usage.

4. CREATE STUDENTS,T=Y,PRVPW=SOCRATES

This example creates the directory STUDENTS on the physical unit specified in the current default directory and enters the name and address of STUDENTS in the current default directory. Only users giving the password SOCRATES are allowed full access rights; others are allowed to LIST the directory STUDENTS and read it when it is part of a pathname, but cannot, for example, make any new entries in the directory.

5. CREATE /MAIN/COURSES/CHINESE/LESSON1, T=P,PRVPW=MING, GRPPW=CHIN,PUBACC=,GRPACC=R

This example is for a new Chinese course to be

stored on the system virtual volume /MAIN. The root directory /MAIN exists, but there are no other files on the disk. In this example, the directories COURSES and CHINESE are implicitly created and the virtual disk LESSON1 is explicitly created. There is no public access to these three files. Users giving the private password MING are given the default private access rights: for the two directories they can create, delete, read, write and erase; and for the virtual disk they can read, write and erase. Users giving the group password, CHIN, can only read the three files.

DELETE

DELETE pathname

-deletes a virtual volume or directory

Parameters and defaults:

pathname: For summary, including password conventions, see PATHNAME, filed alphabetically with commands in this chapter. For discussions, see Section 3.2

Error Messages

29,CURRENTLY MOUNTED OR DEFAULT DIRECTORY

Access Rights Required

E (ERASE) for virtual disk or directory being deleted
D (DELETE) for directory in which it is listed
R (READ) for all directories in pathname

Discussion

The DELETE command:

erases the specified virtual disk or directory and removes its name and address from the parent directory

The DELETE will not be executed if: the file is currently mounted, if the user does not have the required access rights, if it is a directory which is not empty, or if it is the current default directory of any user.

Examples

DELETE ENGLISH.1A:OLDCHAP

This example erases (removes completely) the virtual disk ENGLISH.1A and removes (deletes) its name and address from the current default directory.

HELP

HELP [<subject>]

-displays list of commands or syntax of specified command or format of specified parameter

Parameters and Defaults

[<subject>]

null: lists commands

command word: gives syntax of specified command

parameter: gives format of specified parameter

NET: gives syntax of local commands (SET DRIVEN[,n...] REAL|VIRTUAL [SLOTn][STATION \$nn], SET FS SLOTn[STATION \$nn], SHOW FS, SHOW DRIVES[NOCHECK]. This is available only when entering commands through NET program.

Error Message

19,HELP OPERAND NOT FOUND

Discussion

The user is allowed to enter either ? or HELP when he needs additional information at a user station. Options are (1) HELP, (2) HELP <command word>, (3) HELP <parameter>, (4) HELP NET.

Example

If the user enters:

HELP

the following message is displayed:

ENTER ^HELP [<SUBJECT>]^ WHERE SUBJECT
IS: BLOAD, BSAVE, BRUN, CREATE, DELETE,
LIST, LOCK, UNLOCK, MOUNT, UNMOUNT,
PROTECT, SHOW, PATHNAME, PASSWORD, SET,
NUMBER, SIZE, ACCESS, TYPE, USAGE,
DRIVE, PROTECTION, RENAME, OR TIMESTAMP.

LIST

LIST [pathname] [,VERBOSE] [,NESTED]

-lists entries in directory

Parameters and Defaults

pathname: For summary, see PATHNAME, filed alphabetically with commands in this chapter. For discussion, see Chapter 2.

[,VERBOSE]

if not present, just the names and file types are listed

if present, the names, types and sizes are listed

[,NESTED]

if not present, only entries in the directory addressed by the pathname or current default directory are listed

if present, the system lists

the addressed (or default) directory

all subdirectories whose names appear in the addressed directory

all subdirectories whose names appear in the listed subdirectories, etc. until all directories listed contain only names of virtual or system disks

(the files for each new subdirectory are indented several spaces)

Error Messages

109,ROOT DIR NOT SPECIFIED NO DEFAULT
102,FILE NOT FOUND

Access Rights Required

R (READ) access for each file in pathname

Discussion

This command can be used to list the files in a directory or a family of directories. It is possible to list either the names and types (no VERBOSE), or the names, types and sizes (VERBOSE).

If no pathname is given (e.g. LIST), then the current default directory is listed. If the NESTED or VERBOSE parameters are given when there is no pathname, they must be separated from the word LIST by both a space and comma. For example:

```
LIST ,NESTED
LIST ,VERBOSE
LIST ,NESTED,VERBOSE
LIST
```

Examples

1. LIST /MAIN

The system will display:

LIST

```
/MAIN,T=Y
  BOOTS,T=Y
  SYSTEM,T=Y
  LIB,T=Y
```

The T=Y indicates the files that are directories

2. LIST /MAIN,VERBOSE

The system will display:

```
/MAIN,T=Y,SIZE=3S
  BOOTS,T=Y,SIZE=3S
  SYSTEM,T=Y,SIZE=3S
  LIB,T=Y
```

The size is given in 256-byte sectors.

3. LIST /MAIN,NESTED

```
/MAIN,T=Y
  BOOTS,T=Y
  /APPLE2,T=Y
  BOOT,T=B
  SYSTEM,T=Y
  ERROR,T=S
  HELP,T=Y
    HELP,T=S
    SHOW,T=S
    LIST,T=S
    BRUN,T=S
    LOCK,T=S
    MOUNT,T=S
    BLOAD,T=S
    BSAVE,T=S
    CREATE,T=S
    DELETE,T=S
    UNLOCK,T=S
    UNMOUNT,T=S
    PROTECT,T=S
    SET,T=S
```

PATHNAME, T=S
PASSWORD, T=S
NUMBER, T=S
SIZE, T=S
PROTECTION, T=S
ACCESS, T=S
TYPE, T=S
USAGE, T=S
DRIVE, T=S
LIB, T=Y
APPLE2, T=Y
CPM, T=C
UCSD, T=Y
PASCAL, T=P
DOS, T=D

T=S file system information.

LOCK

LOCK lockname [,usage]

-locks "lockname" for exclusive (EXC) or shared (SHR) use

Parameters and defaults:

lockname:

any arbitrary name (except ALL)
(1-15 characters; no commas, slashes, colons, control characters, carriage returns or unprintable characters; imbedded blanks ok

Acceptable characters: 0-9, A-Z, !, ", #, \$, %, &, ^, (,), *, <, >, ?, [,], {, }, ~, @, _, |

usage:

EXC (exclusive)
SHR (shared)
Default: EXC

Error and Information Messages

40,ILLEGAL LOCK NAME
41,IN USE
42,IN EXC USE

Access Rights Required

None

Discussion

The LOCK command allows users at different terminals to cooperate in using system resources such as individual files or input/output devices. LOCKNAME is any arbitrary name agreed upon by more than one user. For example, if the lock is used to coordinate write access to a given APPLE // DOS file, a program, before writing on that file, would issue a LOCK command. Then, if the return code is 0 indicating no other user station is currently holding the specified lock, the program would proceed to update the file. If, however, the return code is 41 or 42 indicating the lock is currently held at another user station, the program would go into a wait loop or perform some other task before reissuing the LOCK command.

When using locks to protect a particular file, the user should consider the effect of buffering. When a disk write is issued, in some cases the information is transferred to the buffer but not to the disk. One way to make sure it all goes to the disk is to close the file. Buffering can also lead to problems if more than one lock is used for one file, say LOCKA for the first half and LOCKB for the second half; information at the boundary may not be handled correctly.

Therefore, the safest procedure to follow is:

1. Use only one lock for each file.
2. Close the file before issuing the UNLOCK.

Users who wish to use more than one lock per file or avoid closing the file after each write should have a detailed knowledge of exact

LOCK

buffering algorithms used by the current operating system under which the programming is being done.

NOTE: It is not recommended that programs enter a tight wait loop that includes a LOCK command. Instead, they should delay several seconds and then try again. This avoids tying up the network with frequent requests.

See Chapter 4 for a full discussion.

MOUNT pathname, drive [,usage]

- allows user to access a virtual volume to his or her/operating system, as if the volume were inserted in the drive specified.

Parameters and defaults:

pathname: For summary (including password conventions), see PATHNAME, filed alphabetically with commands in this chapter. For discussion, see Chapter 2.

drive:

Dd, where d=number

usage:

RO (READ/ONLY)

RW (READ/WRITE--must have write access)

Default: RO

EXC (exclusive)

SHR (shared)

UPD (RW usage for only one user at a time;
other users may mount the volume RO SHR)

Default: SHR, if RO

UPD, if RW

RO,SHR if no usage parameter
given

Directories (T=Y) and system files (T=S) may only be mounted for read only (RO) access.

MOUNT

Error Messages

30,DRIVE REQUIRED
31,IN USE
32,IN EXC USE
34,RW NOT ALLOWED ON DIRECTORIES
105,NO ACCESS FOR READ TO DIRECTORY
109,ROOT DIR NOT SPECIFIED, NO DEFAULT
111,NO ACCESS FOR WRITE

Access Rights Required

R (read) for virtual disk and all
directories in pathname

W (write) for virtual disk if
being mounted RW

Discussion

The MOUNT command is analogous to inserting a real disk in a floppy disk unit attached to a stand-alone workstation. A MOUNT command sets software pointers so that when a command is given to read or write on a given disk drive, it will address a virtual disk on the file server station.

MOUNT can be reissued on a currently mounted drive, either to change which file is mounted or to change usage modes, without intervening UNMOUNT.

Examples

MOUNT /MAIN/USERS/CAROL/LETTERS,D9,EXC,RW

This command mounts a virtual disk called

LETTERS, which is listed in a subdirectory CAROL, which in turn is listed in a subdirectory USERS, which in turn is listed in the root directory of a system hard disk called MAIN. The virtual disk will be mounted on drive 9; no other user can mount LETTERS until an UNMOUNT command is issued; and Carol can both read and write the files stored on LETTERS. If someone else has already mounted LETTERS, this MOUNT will not be executed; instead an error message

31,IN USE

will be returned.

This example does not specify any passwords. Therefore, it will be executed only if:

there is public read access to all directories and public RW access to the virtual disk LETTERS.

or

the default group or private password gives read access to all directories in the pathname and read and write access to the virtual disk LETTERS.

PATHNAME

pathname: See Section 3.2 for a full discussion.

pathname: /unitname/filepath
or filepath

80 characters max. An initial slash indicates first field is a unit name; no initial slash indicates current default directory is to be prefixed to pathname.

unitname: 1, 2, 3, or 4 [:password]
or name [:password]

filepath: name[:password] [/filepath]

name: name of disk unit, directory, or virtual disk. (1-15 characters; may not include commas, slashes, colons, control characters, carriage returns or unprintable characters; imbedded blanks ok.)

Upper and lowercase can be used for any characters within a file server command and are equivalent.

Control characters are permitted in file server passwords. If the passwords are set or provided by programs running on the network, no difficulty is encountered. However, the presence of serial cards in users and server stations will prevent the console use of some control characters, since these characters have meanings assigned to them by the serial cards.

For example, attempting to type in a password with a particular control character embedded in it might cause the entire console line to be removed.

The following control characters should NOT be used in file server passwords:

A C E F H I J M N R S T V W X Z

Those recommended for use:

B D G K L O P Q U Y

For certain commands a null pathname is allowed:

SET DIR sets current default directory
 to null

LIST lists entries in current
 default directory

PROTECT changes protection parameters
 for current default directory

SHOW PROTECTION displays access rights for
 current default directory

pathname is used in CREATE, DELETE, LIST, MOUNT,
PROTECT, RENAME, SET DIR, SHOW INFO, SHOW
MOUNTS, SHOW PROTECTION.

PROTECT

PROTECT pathname [protection]

-modifies passwords or access rights for a virtual disk or directory

Parameters and defaults:

pathname: For summary, see PATHNAME, filed alphabetically with commands in this chapter. For discussion, see Chapter 2.

[,protection] See Chapter 3 for a detailed discussion.

protection: protect item [,protection]

protect item:

,GRPPW=password
,PRVPW=password
,GRPACC=access rights (Default PUBACC)
,PRVACC=access rights (Default RWECD)
,PUBACC=access rights (Default R)

access rights: set of letters in any order from RWECD (read, write, erase, create, and delete)

Error Messages

11,ILLEGAL PROTECTION PARAMETER
109,ROOT DIR NOT SPECIFIED; NO DEFAULT

Access Rights Required

Private password must be given.
No specific access rights required.

Discussion

The PROTECT command is used to change the password and access rights associated with a given directory or virtual disk. Anyone giving the private password is allowed to use the PROTECT command, regardless of the previously assigned access rights. If there is no private password, then anyone can issue the PROTECT command.

Normally access rights and passwords are set when a directory or virtual disk is created. The PROTECT command allows the user to change them without destroying and recreating the whole file.

A null pathname is allowed. It refers to the current default directory. If the null pathname is used, the comma must still be present, for example:

```
PROTECT ,PRVPW=APRICOTS,PRVACC=RE
```

Note that the PROTECT command does not change the access rights granted to users who have already mounted the virtual disk or directory, or who have a default directory set. The new access rights take effect only for subsequent MOUNT or SET DIR commands.

See Chapter 4 for a full discussion of protection.

Examples

```
PROTECT NANCY,PRVPW=VOLCANO,PRVACC=R,  
PUBACC=,GRPACC=
```

PROTECT

In this example anyone entering the password VOLCANO is allowed to read the virtual disk NANCY, and no one else has any access rights whatsoever. There are no public or group access rights because the protect items PUBACC= and GRPACC= specify no rights. No one can erase or write on this virtual disk until another PROTECT command is issued to assign such rights.

[,protection] See Chapter 3 for a detailed discussion.

protection: protect item [,protection]

protect item:

,GRPPW=password
 ,PRVPW=password
 ,GRPACC=access rights (Default PUBACC)
 ,PRVACC=access rights (Default RWECD)
 ,PUBACC=access rights (Default R)

access rights: set of letters in any order from
 RWECD (read, write, erase,
 create, and delete) used in
 CREATE, PROTECT

RENAME

RENAME oldpathname,newname

-renames specified network volume or directory

Parameters and defaults:

oldpathname: current pathname. For summary, see PATHNAME, filed alphabetically with commands in this chapter. For discussion, see Chapter 2.

newname: last name in pathname is changed to newname

Error Messages

10,PARAMETER TOO LONG
103,BAD DELIMITER IN PATHNAME
105,NO ACCESS FOR READ TO DIRECTORY

Access Rights Required

C, D in parent directory; R for all directories in pathname

Discussion

Renames the specified network volume or directory with 'newname'. The volume or directory to be changed is specified with a complete pathname (beginning with '/') or a partial pathname prefixed by the current default directory. Only the last name in the pathname is changed; do not supply a full pathname for 'newname'. E.g., to change /main/users/abc to /main/users/xyz enter

RENAME /MAIN/USERS/ABC,XYZ

RENAME

A volume or directory file that is currently mounted or set as a default directory may not be renamed. The name of a directory may be changed by supplying the pathname which identifies it. For example, to change /MAIN/USERS/... to /MAIN/PEOPLE/..., enter

```
RENAME /MAIN/USERS,PEOPLE
```

The name of a disk volume can only be changed by using an offline file server utility.

SET DIR

SET DIR pathname

-sets current default directory

Parameters and defaults:

pathname: For summary, see PATHNAME, filed alphabetically with commands in this chapter. For discussion, see Chapter 2.

Error Messages

57, FILE IS NOT A DIRECTORY

Access Rights Required

Read access for all directories in pathname

Discussion

The SET DIR command acts differently depending on whether the specified pathname begins with a slash or not. If the pathname begins with a slash, the default directory is set equal to the specified pathname. But if the pathname doesn't begin with a slash, it is appended to the existing default directory. The last name of the specified pathname must be a directory.

In any subsequent commands, the current default directory is prefixed to pathnames which do not begin with a slash. Passwords may be required in a default directory, and the user is allowed to specify them in the SET DIR command or to use the default private and group passwords set previously by the PRVPW and GRPPW commands.

Access rights for the default directory are determined when the SET DIR is issued.

A SET DIR with no pathname clears the current default directory, i.e. sets it equal to null.

The SET DIR and SET password commands can be combined; for example:

```
SET DIR /MAIN,GRPPW=PINE,PRVPW=CEDAR
```

The delimiter between DIR and pathname can be either a blank or an equal sign.

The SHOW DIR command can be used to display the current default directory (excluding passwords).

Examples

1. SET DIR /1/ACCOUNTS/PAYROLL

This example sets the current default directory equal to the subdirectory PAYROLL which is listed in the subdirectory ACCOUNTS which is listed in the root directory. Now if the command is given to mount the virtual disk SALES

```
MOUNT SALES,D9,RO,SHR
```

it is equivalent to the command:

```
MOUNT /1/ACCOUNTS/PAYROLL/SALES,D9,RO,SHR
```

2. SET DIR SUNNYVALE

Because the pathname in this example does not begin with a slash it is appended to the existing default directory. If this command is issued after the previous example, the resulting default directory would be:

```
/1/ACCOUNTS/PAYROLL/SUNNYVALE
```


SET password

SET [GRPPW=password] [PRVPW=password]

-sets default group or private password

Parameters and Defaults

password: See Chapter 3 for further discussion.

A secret word used to limit access to files (1-15 characters; may not include commas, slashes, colons, carriage returns or unprintable characters; imbedded blanks ok; first character can be any acceptable character)

Error Messages

None specific to setting default passwords

Access Rights Required

None

Discussion

Having to enter a password for each file name takes time and makes it more likely that an unauthorized user will learn the password. Therefore, the PLAN 4000 system allows a user to enter two default passwords, one for private access and one for group access. Then if no password, or an incorrect password, is specified in a pathname, the system will see whether the private or group default password is correct, and, if so, will grant the corresponding access rights.

When a pathname is given, access will be granted under the following conditions:

The access desired is a public access right for the specified file; either no password or an

extraneous password may be specified.

The access desired is a group access right for the specified file, and the correct group password is either specified in the pathname or stored as the default group password, or there is no group password.

The access desired is a private access right for the specified file, and the correct private password is either specified in the pathname or stored as the default private password, or there is no private password.

The SET password and SET DIR commands can be combined; for example:

```
SET DIR /MAIN,GRPPW=PINE,PRVPW=CEDAR
```

Examples

Suppose the teacher in charge of computer assisted mathematics decides he needs a password in order to write a particular disk. All courses have the same private password: OBVIOUS. So, at the beginning of his session, he enters:

```
SET DIR /MATH
SET PRVPW=OBVIOUS
```

Then when he mounts the virtual disk for a given course, say ALGEBRA, instead of typing:

```
MOUNT /MATH:OBVIOUS/ALGEBRA:OBVIOUS,D9,RW,EXC
```

he can shorten it to:

```
MOUNT ALGEBRA,D9,RW,EXC
```

SHOW DATE

SHOW DATE

-displays the current date /MM/DD/YY

Parameters and Defaults

None

Error Messages

None

Access Rights Required

None

Examples

The system displays the current date:

Date is 04/01/83

SHOW DIR

-displays name of current default directory

Parameters and Defaults

None

Error Messages

64,NO DEFAULT DIRECTORY SET

Access Rights Required

None

Discussion

This command displays the pathname of the current default directory. Passwords supplied with a SET DIR are not displayed with SHOW DIR, but they are in effect. SHOW DIR always displays the directory pathname using a unit name rather a unit number.

Example

SHOW DIR

The system displays the current default directory, for example:

/MAIN/USERS/ROOSEVELT

SHOW ID

SHOW ID

-returns the file server identification information:

SERIAL: 0800Annnn00

where nnnn are 4 digits unique to a file server. The complete value represents the file server serial number.

Parameters and Defaults

None

Error Messages

None

Access Rights Required

None

SHOW INFO [pathname]

-SHOW INFO [pathname] gives various information about virtual volumes on a file server disk. The volumes can be any type (directory, binary volume, virtual disk, etc.).

Parameters and Defaults

pathname: enter pathname of virtual volume for which information is desired. You may use the full pathname from the root or any path from the current directory set on your boot volume. If no pathname is supplied, the current default is used.

Error Messages

FILE NOT FOUND

Access Rights Required

READ Access.

Any necessary passwords can be supplied with the pathname.

Discussion

Information provided by SHOW INFO includes:

Volume name

Access rights (public, group, and private)
and presence of passwords

Dates and times of creation, last access,

SHOW INFO

last modification, and last backup

Total size in sectors

Virtual disk type (P, D, etc.)

Volume number (for DOS disks)

For binary (T=B) volumes: the load address and size in bytes (whether or not initialized)

For Apple // DOS (T=D) volumes: the simulated number of sectors per track and tracks per disk (whether or not initialized)

Four dates are stored with each virtual volume (including directories, binary volumes, virtual disks, etc.). The various date/time fields are updated as follows:

<u>Date</u>	<u>When Updated</u>
CREATION	When the volume is first created with the CREATE command
LAST ACCESSED	The first time daily that a volume is mounted or a directory is used.
LAST MODIFIED	The first time after each mount that a volume is written into. If a volume is mounted for RW and never actually written into, this date will not be changed. For directories, this date is changed any time an entry is changed by CREATE, DELETE, or RENAME.

LAST BACKUP When an offline file server utility has been used to make a copy of all or part of a disk, and has been instructed to update the LAST BACKUP dates.

Examples

Suppose that the volume to be displayed has the pathname /MAIN/USERS/ABC/1. A private password, GOLD, has been set, and the default directory is /MAIN. Public and group access rights are restricted to Read. Typing in USERS/ABC/1 will cause a display in some such format as the following (* comments below will not appear):

```

-----/MAIN/USERS/ABC/1 -----
TYPE: P

Pubacc:
Grpacc:
Prvacc: RWECD,PW

Created: YY-MM-DD HH:MM:SS
Access : YY-MM-DD HH:MM:SS
Written: YY-MM-DD HH:MM:SS
Backup : YY-MM-DD HH:MM:SS

Allocated Size: 9999.B (* for T=D,Y,S,B *)
                  9999.S (* for all other types *)

Initialized: Yes (* for T=B,D only *)
Length: 9999 bytes (* for T=B only *)
Loadaddr: $FFFF (* for T=B only *)

Volume: 0 (* for T=D only *)

```


SHOW LOCK

SHOW LOCK lockname

-lists all stations using specified lockname

Parameters and Defaults

lockname

any arbitrary name (except ALL) agreed upon by cooperating users. Has the same restrictions as name: 1-15 characters; may not include commas, slashes, control characters, colons, carriage returns or unprintable characters; imbedded blanks ok; first character can be any acceptable character

Error Messages

2, NAME PARAMETER REQUIRED

Access Rights Required

None

Discussion

The SHOW LOCK lockname command lists the numbers of all stations currently holding the lock called lockname. The station numbers are given in hexadecimal (00 to FF).

Examples

SHOW LOCK PETER

This command will display all the station numbers which currently hold the lock PETER. For example:

04 2F 3C

SHOW [ALL] LOCKS

- displays all locks set at user's own station (or all locks currently held in the file server, with station numbers of the holders).

Parameters and Defaults

None

Error Messages

None specific to SHOW LOCKS

Access Rights Required

None

Discussion

The SHOW LOCKS command lists all locks currently held by a user's own station. SHOW ALL LOCKS lists all locks currently held by any station, together with the numbers of the stations holding the locks.

Examples

1. SHOW LOCKS

This command displays for each lock currently held by a user's own station:

the lockname

whether usage is shared (SHR) or exclusive (EXC)

the number of user stations currently holding the lock.

SHOW [ALL] LOCKS

For example, if the following is displayed:

LOCKA	SHR	2
JILL	EXC	1
DAVID	SHR	1
PETER	SHR	3

it means that one other station currently holds LOCKA for shared usage; only the user's own station holds lock JILL for exclusive usage and lock DAVID for shared usage, and two other stations hold lock PETER for shared usage.

2. SHOW ALL LOCKS

This command displays for each lock currently held in the file server:

the lock name

whether usage is shared (SHR) or exclusive (EXC)

the number of user stations currently holding the lock

the station numbers of the holders

For example, if the following is displayed:

USER.JHM	SHR	1	28
PRINTER	SHR	2	1F
PRINTER	SHR	2	2C
USER.LJS	EXC	1	13

it means that station 28 currently holds lock USER.JHM for shared usage, while stations 2C and 1F hold lock PRINTER for shared usage, and station 13 holds lock USER.LJS for exclusive usage.

SHOW [ALL] MOUNTS

SHOW [ALL] MOUNTS [pathname]

- gives information on virtual disks currently mounted on the file server

Parameters and Defaults

None

Error Messages

131, UNIT NAME NOT FOUND

Access Rights Required

None

Discussion

(a) SHOW MOUNTS

The SHOW MOUNTS command displays for each virtual disk currently mounted by the user's station:

its pathname

its drive number

whether it is read only (RO) or read/write (RW)

whether usage is shared (SHR) or exclusive (EXC), or UPD

its type

its volume number

SHOW [ALL] MOUNTS

its size given in 256 byte sectors (S) for DOS and 512-byte blocks (B) for other operating systems.

SHOW MOUNTS always displays the directory pathname using a unit name rather a unit number.

The file server system uses some sectors for housekeeping information, but these sectors are not counted when the SHOW MOUNT command displays size. However, the LIST command displays a size which may be one sector more than that shown by SHOW MOUNTS.

Examples

(a) SHOW MOUNTS

The system will display:

NAME	DRV	ACCESS	T	VOL	SIZE
/MAIN/LIB/APPLE2/UCSD/PASCAL					
	5	RO SHR P	1	1200B	
/MAIN/USERS/EPS2					
	4	RW EXC P	1	280B	

In some operating system environments, volume numbers are assigned by the user; in other environments, volume number assignment is handled by the operating system. are assigned number 1 by the file server system.

(b) SHOW MOUNTS <pathname>

The SHOW MOUNTS <pathname> command displays the information specified by SHOW MOUNTS for the virtual disk with the given pathname if it is currently mounted by the user's station. Information is not given in nested form, so the

SHOW [ALL] MOUNTS

pathname must be complete. That is, if the user has mounted /MAIN/USERS/JHM/1 and /MAIN/USERS/JHM/2, then the command SHOW MOUNTS /MAIN/USERS/JHM will return a null response; the user must ask explicitly for /MAIN/USERS/JHM/1.

(c) SHOW ALL MOUNTS <pathname>

This command returns information for the virtual volume specified by <pathname>, for every drive/station in the file server network at which it is currently mounted. In addition, station numbers of those stations with the volume currently mounted and total number of stations using the volume are given (STN, USE):

SHOW ALL MOUNTS /MAIN/LIB/APPLE2/UCSD/PASCAL

NAME	DRV	ACCESS	T	VOL	SIZE	STN	USE
/MAIN/LIB/APPLE2/UCSD/PASCAL							
	5	RO SHR	P	1	1800B	20	3
/MAIN/LIB/APPLE2/UCSD/PASCAL							
	5	RO SHR	P	1	1800B	07	3
/MAIN/LIB/APPLE2/UCSD/PASCAL							
	5	RO SHR	P	1	1800B	1E	3

SHOW PROTECTION

SHOW PROTECTION [pathname]

- displays group, private and public access rights for file addressed by pathname

Parameters and Defaults:

pathname: See PATHNAME, filed alphabetically with commands in this chapter and Chapter 2.

Error Messages

64,NO DEFAULT DIRECTORY SET
110,NO ACCESS FOR READ

Access Rights Required

R (READ) access for every file in pathname

Discussion

This command can be abbreviated to

SHOW PROTECT [pathname]

It displays public, group and private access rights for the specified file (or default directory if no pathname is specified). Passwords are never displayed, but the existence of passwords is indicated by "PW".

Example

SHOW PROTECT /MAIN/USERS/NSS/2

PUBACC=R
GRPACC=R
PRVACC=RWE, PW

When this virtual disk was created, no usage rights were specified, so that the system defaults are in effect. However, a private password was set, so that access to the volume is READ/ONLY unless the password is given.

SHOW STATION

SHOW STATION

-displays the number of the user station

Parameters and Defaults

None

Error Messages

None

Access Rights Required

None

Examples

SHOW STATION

The system displays the hexadecimal user station number, for example:

STATION IS \$07

SHOW TIME

SHOW TIME

-Returns current date and time

Parameters and Defaults

None

Error Messages

None

Access Rights Required

None

Examples

SHOW TIME

This command returns

80,Day DD-Mon-19YY HH:MM:SS

SHOW TYPE

SHOW TYPE drive

- displays type of virtual disk mounted on drive d

Parameters and Defaults

drive Dd, where d=number

See user operating system guides for details on drives.

Error Messages

59,TYPE=SYSTEM
61,DRIVE REQUIRED
62,NOT CURRENTLY MOUNTED
63,TYPE=APPLE // CPM
65,TYPE=APPLE // PASCAL
66,TYPE=APPLE // DOS
67,TYPE=BINARY
68,TYPE=DIRECTORY
69,UNKNOWN TYPE
73,TYPE=TEXT
74,TYPE=APPLE /// SOS
75,TYPE=IBM PC DOS
76,TYPE=IBM PC PASCAL

Access Rights Required

None

Discussion

This command is used to determine the type of a given file. Its main use is by BOOT programs which must determine the type of volume that the user has specified as volume to boot.

SHOW TYPE

Examples

SHOW TYPE D4

The system responds:

65,TYPE=APPLE // PASCAL

SHOW TYPES

SHOW TYPES

- displays types of virtual disks mounted on drives 1-16

Parameters and Defaults:

None

Error Messages

None

Access Rights Required

None

Discussion

Returns the types of virtual disks (Y, P, D, B, C, 3, I, T, U) currently mounted on drives 1-16. The information appears in a string, as shown in the example below. A dash, "-", indicates that nothing is mounted on the drive.

Example

SHOW TYPES

The system responds:

71,---PP---P-PP----

showing that the station has virtual Apple // Pascal disks mounted on drives 4, 5, 9, 11, and 12.

SHOW VOLS

- displays the currently active physical disk drive names and numbers.

Parameters and Defaults

None

Error Messages

None

Access Rights Required

None

Examples

SHOW VOLS

The system displays the current disk drives, for example:

```
DISK UNIT 1 IS /MAIN
DISK UNIT 2 IS /SPARE
0,OK
```

TIMESTAMP

TIMESTAMP

-returns encoded form of the current date and time

Parameters and Defaults

None

Error Messages

None

Access Rights Required

None

Discussion

Returns encoded form of the current date and time. Format of the returned message is 70,yyymmddhhmmssw where yy is current year (e.g., 81) mm is current month, dd is current date, and hhmmss are the current time. 'w' is the day of the week (Sunday is 1).

UNLOCK lockname or UNLOCK ALL

-releases locked usage on a lockname
or on all locknames currently held

Parameters and Defaults

lockname

any arbitrary name agreed upon (except ALL)
(1-15 characters; no commas, slashes, colons,
carriage returns or unprintable characters;
imbedded blanks ok, first character any
acceptable character)

Error Messages

45,NOT HELD

Access Rights Required

None

Discussion

The UNLOCK command frees a lock on an agreed upon lockname, so that users at other terminals know it is all right now to access a file, external device, or other resource.

Examples

1. UNLOCK AMY

This command unlocks the lock called Amy.

2. UNLOCK ALL

This command unlocks all locks currently held by a user's own station.

UNMOUNT

UNMOUNT drive or UNMOUNT ALL

-cancels previous mount(s)

Parameters and Defaults

drive

Dd, where d=number (either \$hex or decimal)

See user operating system guides for details on drives.

Error Messages

35,DRIVE OR "ALL" REQUIRED

36,NOT CURRENTLY MOUNTED

Access Rights Required

None

Discussion

It is not necessary to do an UNMOUNT before mounting the same or a different virtual disk on a given drive. UNMOUNT is useful primarily to protect a virtual disk mounted with read/write access from accidental writes after it is no longer needed.

WARNING: if a Apple // Pascal user issues a command to

UNMOUNT ALL

the Pascal system on that Apple will crash since

UNMOUNT

there is no longer any booted volume on line. It will be necessary to turn power off and on to recover. Therefore, UNMOUNT ALL should never be given in Apple // Pascal, unless immediately followed by appropriate reMOUNTs.

Examples

UNMOUNT D9

This command resets the pointers which caused disk commands to read and write to a specified virtual disk whenever drive 9 was addressed.

Appendix A

Error and Information Messages

When the file server receives a file server command from a user station, it executes the command, if possible, and, in any case, returns two variables:

- return code - an integer between 0 and 200
- return message, such as OK, ILLEGAL COMMAND, or TYPE=PASCAL

Messages are of several types:

- information, such as OK, IN USE, TYPE=BINARY
- user errors such as syntax errors or attempting to access a Network file without the necessary access rights
- system errors such as memory full or disk full; these should be reported to the system manager.

In this list, messages are classified as:

general syntax

pertaining to a specific command

system errors

file system errors.

ERRORS

General Syntax (0-19)

0,OK

(Not an error.) The command was syntactically correct and was executed without error.

1,ILLEGAL COMMAND

The command verb cannot be recognized, or cannot be executed from this user station operating system environment. The command verb is the first word of the command, and must be separated from the rest of the command with one or more blanks.

2,NAME PARAMETER REQUIRED

The first parameter of the command must be a non-null pathname.

3,UNRECOGNIZED PARAMETER

A keyword parameter was not recognized. Check the spelling carefully, and make sure that it is properly separated from the previous and following items with commas.

4,ILLEGAL DRIVE NUMBER

A drive number must be specified with "D" followed by an integer in the range supported for your environment. Example: "D4".

5,ILLEGAL STATION NUMBER

A station number must be specified as a two-digit hexadecimal number preceded with \$, in the range \$1 to \$FE. Example: "\$2D".

7,PARAMETER APPEARS TWICE

A keyword parameter appears more than once in a single command. There can only be one occurrence of a keyword parameter, even if multiple occurrences have the same value.

8,ILLEGAL TYPE PARAMETER

The "T=" value is not one of the legal volume types. It must be one of the following:

P (Apple // Pascal)	B (binary)
D (Apple // DOS),	S (system)
C (Apple // CP/M)	Y (directory)
3 (Apple /// SOS)	T (text)
U (IBM PC p-SYSTEM PASCAL)	I (IBM PC DOS)

Example: T=P

9,COMMAND TOO LONG

A file server command must be no longer than 80 characters. In unusual cases where this is a problem, long commands can often be shortened by using a default directory, or by assigning access rights in a subsequent PROTECT command.

10,PARAMETER TOO LONG

The new name given as the second parameter of the RENAME command must be no more than 15 characters long. Remember that RENAME changes only the last name in the sequence of names which constitute a pathname. If you wish to change the name of a directory, give the pathname of the directory itself as the first parameter of RENAME.

ERRORS

11,ILLEGAL PROTECTION PARAMETER

The value of the PUBACC, GRPACC, or PRVACC protection item is incorrect. The value must be some combination of the letters RWECD (read, write, erase, create, and delete), or may be null. For example, "GRPACC=RW" or "PUBACC=".

12,NO STATION CMD; USE \$NN PREFIX

The "station" command has been removed. Use "\$nn <command>" where nn is the station number on whose behalf you wish to issue the command. (file server console only.)

13,ILLEGAL NUMBER (NEGATIVE OR TOO BIG)

The number was less than 0 or bigger than 32767. Number may be specified in decimal, or in hexadecimal preceded by \$. Examples: "42", "\$1A3".

19,HELP FILE NOT FOUND

There is no HELP file for the word used as an operand of the HELP command. Use the HELP command with any parameters to see what the possible HELP parameters are. (The system manager has the option of removing all HELP files to save space.)

Create (20-25)

20,TYPE PARAMETER REQUIRED (T=?)

The type parameter was missing. Example:"T=D".

21,SIZE OUT OF RANGE (<0B OR >32752B)

The value of the SIZE parameter was negative or greater than 32752 blocks. Each block is 512 bytes. Other units that can be specified are C (characters), and K (1024 bytes). If the units are omitted, B (512-byte blocks) is assumed. Examples: "SIZE=280", "SIZE=2000S".

23,SIZE PARAMETER REQUIRED WITH T=B, =T

The SIZE parameter must be specified to create a binary volume. The size may be an overestimate of the size of the data to be BSAVED into the volume, but it must not be less.

24,SIZE OUT OF RANGE (<1C OR >48K)

The limits on the size of a binary (T=B) file are between 1C (one byte) and 48K (49152 bytes) regardless of the units used in the specification.

Delete (25-29)

29,CURRENTLY MOUNTED OR DEFAULT DIR

You cannot delete a volume which is currently mounted by any station, or which is the default directory (see the SET DIR command) of any station.

Mount (30-34)

30,DRIVE REQUIRED

You must specify what drive the volume is to be mounted on. Example: "D4".

ERRORS

31,IN USE

The volume you asked to mount is in use by another station. You are therefore denied exclusive use of that volume.

32,IN EXC USE

The volume you asked to mount is in exclusive use by another station. You are therefore denied any use of the volume.

34,RW NOT ALLOWED ON DIRECTORIES

You are not allowed to mount a directory (T=Y) volume for write access.

Unmount (35-39)

35,DRIVE OR "ALL" REQUIRED

You must specify a drive number or "ALL" on the UNMOUNT command. Examples: "UNMOUNT D1", "UNMOUNT ALL".

36,NOT CURRENTLY MOUNTED

The drive number specified in the UNMOUNT command does not have any virtual volume mounted on it by the file server.

Lock (40-44)

40,ILLEGAL LOCK NAME

A lock name must be 1 to 15 characters long.

41, IN USE

The lock name specified is in use by another station. You are therefore denied exclusive use of the lock.

42, IN EXC USE

The lock name specified is in exclusive use by another station. You are therefore denied any use of the lock.

Unlock (45-49)

45, NOT HELD

The lock name specified is not currently held by your station.

BSAVE, BRUN, BLOAD (50-55)

50, CMD NOT ALLOWED FROM THIS STATION

The BSAVE/BLOAD/BRUN/OFF commands may only be executed from an Apple // user station.

51, NOT BINARY

The pathname identifies a volume which is not binary (T=B). Only binary volumes can be used for BSAVE, BLOAD, or BRUN commands.

52, NOT PREVIOUSLY SAVED

The binary volume was created but has never had any data written into it using the BSAVE command. It can not be used with BLOAD or BRUN until it has been BSAVED into.

ERRORS

53, FROM PARAMETER REQUIRED

For BSAVE, the FROM parameter, which specifies the memory area from which data is to be taken, must be provided. Example: "FROM=\$1000".

54, SIZE PARAMETER REQUIRED

For BSAVE, you must provide the SIZE parameter on the BSAVE command to indicate how much data is to be saved. This value must be less than or equal to the size of the volume specified on the original CREATE command. Example: "SIZE=256.C".

55, FILE WAS THERE; REP NOT SPECIFIED

Data has already been saved in the binary volume. To replace that data, you must specify "REPLACE" as a parameter in the BSAVE command.

Set/List (57-58)

57, FILE IS NOT A DIRECTORY

The pathname given in a SET DIR command identifies a volume which is not a directory (T=Y).

58, USE: SET TIME [YYMMDD] [,HH[MM]]

If the date parameter was supplied, it was incomplete or contained invalid fields. If the time of day parameter was supplied, it contained invalid fields.

Show (59-69)

59,TYPE=SYSTEM

(Not an error.) The volume mounted on the drive for which you did a "SHOW TYPE" is a system volume (T=S).

60,SHOW OPTION NOT RECOGNIZED

The operand of a "SHOW" command was not recognized. Check the spelling and make sure there are no extraneous items in the command.

61,DRIVE REQUIRED

For the "SHOW TYPE" command you must specify the drive number on which the volume is mounted. Example: "SHOW TYPE D12".

62,NOT CURRENTLY MOUNTED

The drive number specified has no volume mounted on it by the file server.

63,TYPE=APPLE // CP/M

(Not an error.) The volume mounted on the drive for which you did a "SHOW TYPE" is an Apple // CP/M volume. (T=C).

64,NO DEFAULT DIRECTORY SET

(Not necessarily an error.) This response to the "SHOW DIR" command indicates that there is no default directory established for this station by the file server.

ERRORS

65,TYPE=APPLE // PASCAL

(Not an error.) The volume mounted on the drive for which you did a "SHOW TYPE" is an Apple // Pascal volume (T=P).

66,TYPE=APPLE // DOS

(Not an error.) The volume mounted on the drive for which you did a "SHOW TYPE" is an Apple // DOS volume (T=D).

67,TYPE=BINARY

(Not an error.) The volume mounted on the drive for which you did a "SHOW TYPE" is a binary volume (T=B).

68,TYPE=DIRECTORY

(Not an error.) The volume mounted on the drive for which you did a "SHOW TYPE" is a directory (T=Y).

69,UNKNOWN TYPE

The volume mounted on the drive for which you did a "SHOW TYPE" is not a standard volume type.

70,yyymmddhhmmssw

(Not an error.) Returns date and time information in encoded form. For example, the FS command `TIMESTAMP` returns the current year, month, day, hour, minute, second, and day of the week in the form 70,8104301859381 (that is, 6:59 P.M., Sunday, April 30, 1981).

71,--t--tt--t-t----

(Not an error.) Returns types of virtual disks currently mounted on drives 1-16 (Y,P,D,B,S,C,3,I,U,T). The system responds to the FS command SHOW TYPES using this format.

72,TODAY IS DD-MON-YYYY HH:MM:SS

(Not an error.) This is the response to the SHOW TIME command.

73,TYPE=TEXT

(Not an error.) The volume mounted on the drive for which you did the SHOW TYPE is a text volume (T=T).

74,TYPE=APPLE /// SOS

(Not an error.) The volume mounted on the drive for which you did the SHOW TYPE is an Apple /// SOS volume (T=3).

75,TYPE=IBM PC DOS

(Not an error.) The volume mounted on the drive for which you did the SHOW TYPE is an IBM PC DOS volume (T=I).

76,TYPE=IBM PC P-SYSTEM PASCAL

(Not an error.) The volume mounted on the drive for which you did a "SHOW TYPE" is an IBM PC p-System Pascal volume (T=U).

ERRORS

Local Commands (90-92)

Vary according to user environment. See the appropriate User Guide.

System Errors (94-99)

94,NOT CONNECTED

This is a network error that indicates that the connection to another station has been terminated prematurely.

95,UNRECOGNIZABLE NETWORK RESPONSE

The last response message from file server did not contain a numeric error code, as expected. This may indicate incorrect logic in the use of NETUNIT procedures from within Pascal programs.

96,NO NETWORK CARD IN SLOT

The slot number specified does not have a Nestar network interface card installed, or the card is defective.

97,FILE SERVER MEMORY FULL

The file server has no space left for tables needed to complete your request. This does NOT refer to memory space in the user station.

98, NETWORK ERROR

The network routines were unable to complete the transaction. The error may be transient; see the description of NETUNIT for more information. This error does not occur from most user level programs, such as NET.

99, USER ABORT

The network abort key was pressed while a network transaction was queued up or in progress. The transaction was aborted.

File System Errors (100-140)

101, END OF FILE OR RECORD OUT OF RANGE

An attempt was made to read a block or sector of a volume which is outside the legal range for that volume.

102, FILE NOT FOUND

The volume specified by the pathname was not found, or one of the directories in the pathname was not found. Check the spelling of each filename in the pathname. If the name does not begin with a slash, check that the current default directory is the correct one.

103, BAD DELIMITER IN PATHNAME

A delimiter other than "/" or ":" was found in a pathname. Make sure that you have not omitted a comma separating the pathname from other operands in the command.

ERRORS

104, FILE NAME OR PASSWORD TOO BIG

A single filename (the part between slashes in a pathname), or password (the part after a colon in a pathname) is longer than the maximum of 15 characters.

105, NO ACCESS FOR READ TO DIRECTORY

You have been denied read access to a directory which is part of the specified pathname.

106, NON DIRECTORY FOUND IN PATHNAME

One of the names in the pathname (other than the last name) identifies a volume which is not a directory (T=Y). Only the last thing in a pathname can be other than a directory.

107, END OF PATHNAME IS A DIRECTORY

The pathname specifies a directory (T=Y) in a context where a non-directory volume is required.

109, ROOT DIR NOT SPECIFIED NO DEFAULT

The specified pathname does not begin with a slash, and there is no default directory recorded for this station by the file server. If you wish to completely specify the pathname, begin with a slash and the name or number of the disk unit. If you wish to use the current default directory, do not begin the pathname with a slash. You may use the "SHOW DIR" command to find out the current default directory, and the "SET DIR" command to establish one.

110,NO ACCESS FOR READ

You have been denied read access to the volume specified by the pathname, or to a directory along the path.

111,NO ACCESS FOR WRITE

You have been denied write access to the volume specified by the pathname.

112,NO ACCESS FOR APPEND (not yet implemented)

You have been denied append access to the volume specified by the pathname.

113,NO ACCESS FOR ERASE

You have been denied erase access to the volume specified by the pathname. Erase access is necessary to delete the file.

114,NO ACCESS FOR CREATE

You have been denied access to create or rename an entry in one of the directories specified in the pathname.

115,NO ACCESS FOR DELETE

You have been denied access to delete or rename an entry in one of the directories specified in the pathname.

ERRORS

116,CANT DELETE NON-EMPTY DIRECTORY

The pathname specified in a DELETE command identifies a directory, and that directory is not empty, that is, it still points to other volumes. Only empty directories can be deleted by a single file server DELETE command. To delete non-empty directories (i.e. subtrees) see the description of the TREEWALK utility in the User's Manual for supported environments.

117,FILE SERVER MEMORY FULL

The file server has no space left for tables needed to complete your request. This does NOT refer to memory space in the user station.

118,DISK FULL

There is not enough contiguous space left on the disk unit to create the volume. The LIST command when used to display the root directory will give information about the space available on a disk unit. Example: "LIST /MAIN".

119,DIRECTORY FULL

There is not enough space left to create more entries in the directory, and the directory cannot be expanded. Directories are automatically expanded as necessary to accomodate new entries.

120,INTERNAL ERROR

An internal error has been detected by the file server. Additional information is written on the console of the file server. That information and the circumstances surrounding the error should be transmitted to your support organization for diagnosis. The file server should be restarted as soon as practical.

121, UNINITIALIZED DISK

The disk unit has not been initialized. All disks must be formatted and initialized using the file server FORMAT DISK utility; see the File Server Installation and Operation Manual.

122, WRONG SOFTWARE VERSION

The disk format is not compatible with version of the file server currently running. (This error cannot occur with any file servers so far released.)

123, FILE ALREADY EXISTS

The file you have asked to create, or the new name used in a RENAME command, already exists in the directory.

124, DISK I/O ERROR, SUBCODES x,y

A hardware I/O error was detected. The details of the error are described in the subcodes; for more information see the table of I/O errors in Appendix A of the File Server Installation and Operation Manual.

125, VERIFY FAILED (BAD MEMORY)

All disk write operations are verified by reading back the recorded data and comparing it to the data stored in memory. This error indicates that the disk data did not compare correctly. It sometimes indicates a memory error in the file server, and not a disk error.

128, BAD UNIT NUMBER IN PATHNAME

The first item after the initial slash in a pathname is a number, but it is not in the legal range for unit numbers (1 to 4).

ERRORS

130, NEED PRIVATE PASSWORD FOR PROTECT

In order to execute the PROTECT command for any volume, the private password must be specified in the pathname or as a default private password. The password must be specified whenever the volume has a non-null private password, regardless of the access rights currently assigned to the volume.

131, UNIT NAME NOT FOUND

The name after the initial slash of a pathname is not the name of a disk unit currently recognized by the file server. You can also use the unit number in place of a name, if you wish.

133, DISK NOT READY

The disk unit specified is not ready. The one minute warmup period after initial power up may not have elapsed. It may also indicate a controller or disk drive failure.

A

access rights
 default 3-7
 network commands 3-10
 passwords 3-5

B

bibliography BB-1
binary commands, access 3-11
blanks, in pathnames 2-8, 5-1

C

characters, in pathnames 2-7
commands, file server 5-1
 syntax 5-4
control characters, pathnames 2-9
CREATE access 3-3, 3-9
CREATE command 5-5
creating virtual volumes 1-2, 5-5

D

default access rights 3-7
default directory: 2-9
DELETE access 3-3, 3-9
DELETE commands 5-14
directories 1-1, 2-3
disclaimer ii
disk organization 2-1

INDEX

disk units: 2-1, 2-4

E

encryption 3-12

ERASE

access 3-3

error messages A-1

EXC 3-2

exclusive usage 3-2

F

fields 5-2

file server commands 1-2, 5-1

file servers 1-1, 2-3

file structure 2-2

files 2-2

G

group password 3-5

group usage 3-3

GRP 3-3

GRPACC 3-5

GRPPW 3-5

H

HELP 5-16

K

keyword 5-2

L

limits on size 5-7

LIST 5-18

LOCK 4-1, 5-22

lock command 4-1

locks 4-1ff

M

/MAIN 2-2, 2-4

MOUNT 5-25

usage modes with 3-12

"mounting" virtual volumes 1-2

N

nested directories 1-1

NET program 1-2

network operation 1-1

null pathname 2-2

O

operation, network 1-1

P

INDEX

PATHNAME 5-28

pathname

 formal definition 2-7

 /unitname 2-5

 /unitname/directory 2-6

 /unitname/directory1/directory2/ 2-6

 /unitnumber 2-5

 virtual volume 2-6

pathnaming conventions 2-1, 2-4ff

passwords 2-10, 3-1, 3-5, 3-9

 forgetting 3-12

preset passwords 3-9

private password 3-5

private usage 3-3, 3-5

PROTECT 3-8, 5-30

protection 3-1ff, 5-48

PRV 3-3

PRVACC 3-5

PRVPW 3-5

PUB 3-3

PUBACC 3-5

public usage 3-3, 3-5

R

READ access 3-3

RENAME 5-34

root directory 2-2, 2-5

S

server stations 1-1

SET DIR 5-36

SET password 5-38

SHOW DATE 5-40

SHOW DIR 5-41

SHOW ID 5-42
 SHOW INFO 5-43
 SHOW LOCK 5-46
 SHOW LOCK(S) 4-3
 SHOW [ALL] LOCKS 5-47
 SHOW [ALL] MOUNTS 5-49
 SHOW PROTECTION 3-8, 5-52
 SHOW STATION 5-54
 SHOW TIME 5-55
 SHOW TYPE 5-56
 SHOW TYPES 5-58
 SHOW VOLS 5-59
 shared usage 3-2
 SHR 3-2
 size, volume 5-7
 limits 5-7
 subdirectories 2-3, 2-4, 2-6
 system volumes 2-3

T

TIMESTAMP: 5-60
 type, volume 5-7

U

unit name 2-5
 units 2-1, 2-4
 UNLOCK 4-2, 5-61
 UNMOUNT 5-62
 UPD 3-2
 "update" usage 3-2
 usage 3-lff
 with LOCK 4-1
 with MOUNT 3-12
 with other commands 3-10
 user classes 3-3

INDEX

V

version number, file server iii
virtual diskettes 1-1ff, 2-1, 2-3, 2-4
virtual volumes 1-1ff, 2-1, 2-3, 2-4
volume names 2-1
 size 5-7
 type 5-7

W

WRITE access 3-3

BIBLIOGRAPHY

PLAN 4000 PUBLICATIONS

General Information Manual	GA40-0100
PLAN 4000 Physical Planning and Installation Manual	GA40-0101
File Server User's Manual	SC40-0200
File Server Apple // Pascal User's Guide	SC40-0501
File Server Apple // DOS User's Guide	SC40-0502
File Server Apple // CP/M User's Guide	SC40-0503
File Server Apple /// SOS User's Guide	SC40-0504
File Server IBM PC DOS User's Guide	SC40-0505
File Server IBM PC UCSD p-System User's Guide	SC40-0506
File Server Installation and Operation Manual	SC40-0300
PLAN 4000 System Service Manual	LA40-0401
Print Server User's Manual	SC40-0201
Print Server Installation and Operation Manual	SC40-0301
Messenger User's Manual	SH40-0204
Messenger Installation and Operation Manual	SH40-0304



Reader Comment Form

This manual is one in a series that describes the use of the PLAN 4000 system.

You are encouraged to use this form to communicate to Nestar any problems or suggestions associated with the system. We would like your comments on improving the system itself, as well as on this documentation. Possible topics for comment are: clarity, accuracy, completeness, organization, coding, retrieval and legibility.

No postage stamp is necessary if mailed within the U.S.A.

Nestar installation location:

Submitter's name :

Address :

Description of problem or suggestion:

Please mail this form to :

Nestar Systems, Incorporated
2585 E. Bayshore Road
Palo Alto, California 94303
Attn: PUBLICATIONS DEPT.



No Postage
Necessary
If Mailed
In The
United States

BUSINESS REPLY CARD

First Class

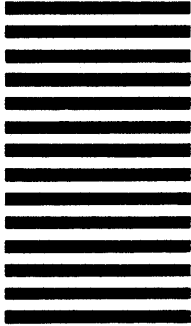
Permit No. 239

Palo Alto, CA

POSTAGE WILL BE PAID BY ADDRESSEE

NESTAR SYSTEMS
INCORPORATED

2585 East Bayshore Road
Palo Alto, California 94303



Fold here

Please do not staple

Tape

Reader Comment Form

This manual is one in a series that describes the use of the PLAN 4000 system.

You are encouraged to use this form to communicate to Nestar any problems or suggestions associated with the system. We would like your comments on improving the system itself, as well as on this documentation. Possible topics for comment are: clarity, accuracy, completeness, organization, coding, retrieval and legibility.

No postage stamp is necessary if mailed within the U.S.A.

Nestar installation location:

Submitter's name :

Address :

Description of problem or suggestion:

Please mail this form to :

Nestar Systems, Incorporated
2585 E. Bayshore Road
Palo Alto, California 94303
Attn: PUBLICATIONS DEPT.



No Postage
Necessary
If Mailed
In The
United States

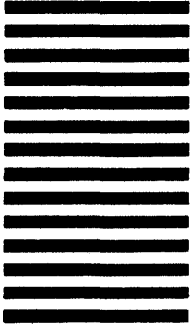
BUSINESS REPLY CARD

First Class

Permit No. 239

Palo Alto, CA

POSTAGE WILL BE PAID BY ADDRESSEE



NESTAR SYSTEMS
INCORPORATED

2585 East Bayshore Road
Palo Alto, California 94303

Fold here

Please do not staple

Tape