DataGeneral
Data General Corporation, Westboro, Massachusetts 01580

Customer Documentation

NetWare® for AViiON® Systems: Installation

069–000488–06

AViiON®
PRODUCT LINE

NetWare® for AViiON® Systems: Installation

069–000488–06

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

Printed in the United States of America
Rev. 06, June 1994

Ordering No. 069–000488

Notice

DATA GENERAL CORPORATION (DGC) HAS PREPARED AND/OR HAS DISTRIBUTED THIS DOCUMENT FOR USE BY DGC PERSONNEL, LICENSEES, PROSPECTIVE CUSTOMERS, AND CUSTOMERS. THE INFORMATION CONTAINED HEREIN IS THE PROPERTY OF THE COPYRIGHT HOLDER(S); AND THE CONTENTS OF THIS MANUAL SHALL NOT BE REPRODUCED IN WHOLE OR IN PART NOR USED OTHER THAN AS ALLOWED IN THE APPLICABLE LICENSE AGREEMENT.

The copyright holder(s) reserve the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases determine whether any such changes have been made.

THE TERMS AND CONDITIONS GOVERNING THE SALE OF DGC HARDWARE PRODUCTS AND THE LICENSING OF DGC SOFTWARE CONSIST SOLELY OF THOSE SET FORTH IN THE WRITTEN CONTRACTS BETWEEN DGC AND ITS CUSTOMERS, AND THE TERMS AND CONDITIONS GOVERNING THE LICENSING OF THIRD PARTY SOFTWARE CONSIST SOLELY OF THOSE SET FORTH IN THE APPLICABLE LICENSE AGREEMENT. NO REPRESENTATION OR OTHER AFFIRMATION OF FACT CONTAINED IN THIS DOCUMENT INCLUDING BUT NOT LIMITED TO STATEMENTS REGARDING CAPACITY, RESPONSE–TIME, SUITABILITY FOR USE OR PERFORMANCE OF PRODUCTS DESCRIBED HEREIN SHALL BE DEEMED TO BE A WARRANTY BY DGC FOR ANY PURPOSE, OR GIVE RISE TO ANY LIABILITY OF DGC WHATSOEVER.

IN NO EVENT SHALL DGC BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS DOCUMENT OR THE INFORMATION CONTAINED IN IT, EVEN IF DGC HAS BEEN ADVISED, KNEW OR SHOULD HAVE KNOWN OF THE POSSIBILITY OF SUCH DAMAGES.

All software is made available solely pursuant to the terms and conditions of the applicable license agreement which governs its use.

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

Data General Corporation
4400 Computer Drive
Westboro, MA 01580

NetWare® for AViiON® Systems: Installation

069-000488-06

Revision History:		Effective with:
Original Release	– May 1990	
First Revision	– November 1990	
Second Revision	– October 1991	
Third Revision	– May 1992	
Fourth Revision	– October 1992	
Fifth Revision	– May 1993	
Sixth Revision	– June 1994	DG/UX 5.4R3.00 and 5.4R3.00T NetWare® 3.11 for AViiON® Systems, Rev. 3.00

A vertical bar in the margin of a page indicates substantive technical change from the previous revision except for Appendix D, which is entirely new.

About this manual

This manual shows you how to install the NetWare® for AViiON® Systems product. It also helps you establish network directories, and set up user accounts.

NetWare is a network of computers that lets users exchange information with other users on the network, and use the filing and printing resources available on the network.

A NetWare network can incorporate mainframe computers, backup devices, and different types of servers, (such as print servers and archive servers).

This manual is for NetWare network system administrators, or anyone who must get the NetWare network up and running for the first time or upgrade the network. To use this manual, you should be experienced with PC hardware and software, and be familiar with NetWare terminology and concepts. We assume that you are familiar with both the UNIX® and MS–DOS® operating systems. You should also be acquainted with the AViiON server and DG/UX™ operating system, which will run the host software. We assume that you have your AViiON and PC or Macintosh® workstations installed and running correctly.

How this manual is organized

The following list gives an overview of what you will find in the chapters and appendices of this manual:

Chapter 1 **Getting Started** Leads you through the steps required to plan your NetWare for AViiON Systems network.

Chapter 2 **Installing NetWare on a New or Existing System** Explains installing NetWare for AViiON Systems for the first time or on an existing NetWare system. It also tells how to use **pconfig** to configure DG/UX printers to the NetWare network.

Chapter 3 **Router Installation and Management** Explains installing and managing a dedicated or nondedicated router.

Chapter 4 **Network File Services Setup** Provides guidelines for planning and creating your network environment.

Appendix A **Login Script Commands** Gives an alphabetical listing of the login script commands.

Appendix B **Installation Worksheets** Contains blank and sample filled–in installation worksheets.

Appendix C **Installing NetWare for AViiON Systems on a Trusted DG/UX System** Explains installing NetWare for AViiON Systems on a Trusted DG/UX System. NetWare on a Trusted DG/UX System has security features available only on a DG/UX Trusted system.

Appendix D **Installing and Using High Availability Features with NetWare** Gives an overview of two high availability methods: multi–path LAN I/O and server failover. It also describes installing NetWare with server failover, modifying server failover with scripts, and setting up NetWare to continue printing after a system failover.

Related Data General manuals

Within this manual, we refer to the following manuals for information about Novell Netware products:

NetWare® for AViiON® Series Systems: Concepts (069–000483) For all levels of NetWare users, this manual provides an alphabetically arranged glossary of NetWare terminology. It will be particularly useful to supervisors who are performing their first installation of the NetWare for AViiON Systems product.

NetWare® for AViiON® Series Systems: System Administration (069–000487) For network supervisors who will use SCONSOLE to administer the AViiON file server.

NetWare® for AViiON® Series Systems: Utilities (069–000484) For all levels of network users, this manual provides an alphabetically arranged reference for NetWare command line and menu utilities.

NetWare® for AViiON® Series Systems: User Book (069–000486) For first–time users who are unfamiliar with networks, this manual provides a general overview of NetWare.

NetWare® for AViiON® Series Systems: System Messages (069–000485) For all levels of Network users, this manual contains solutions to common network problems and advice on preventing problems. It lists NetWare system messages alphabetically, citing a cause and recommended action for each.

NetWare® for AViiON® Series Systems: Print Server (069–000706) For the network supervisor, this manual describes how NetWare printing works, how to install and run a print server, and how to use printing utilities.

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

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

If you are unfamiliar with any DG/UX procedure described in this manual, you can find explanations in the manuals:

Installing the DG/UX™ System (093–701087)

Customizing the DG/UX™ System (093–701101)

For information about managing the DG/UX system, see

Managing the DG/UX™ System (093–701088)

For information related to Trusted NetWare for AViiON Systems and Trusted DG/UX features and processes, see

Trusted Facility Manual for the B1 Trusted DG/UX™ System (093–701114)

Trusted Facility Manual for the C2 Trusted DG/UX™ System (093–701110)

Audit System Administrators Guide for the B1 Trusted DG/UX™ System (093–701115)

Audit System Administrators Guide for the C2 Trusted DG/UX™ System (093–701111)

If you are unfamiliar networks, you may want to read "Introduction to NetWare" in *NetWare® for AViiON® Systems: User Basics* (069–000486) before reading this manual.

For information about high availability systems, see

Achieving High Availability on AViiON Systems (093–701133)

If you are unfamiliar with high–availability systems, read this manual for an overview of the hardware and software components that provide highly available AViiON systems. Included are a set of scenarios with specific examples of how to set up and run high–availability systems.

Reader, please note:

Data General manuals use certain symbols and styles of type to indicate different meanings. The Data General symbol and typeface conventions used in this manual are defined in the following list. You should familiarize yourself with these conventions before reading the manual.

This manual also presumes the following meanings for the terms "command line," "format line," and "syntax line." A command line is an example of a command string that you should type verbatim; it is preceded by a system prompt and is followed by a delimiter such as the curved arrow symbol for the New Line key. A format line shows how to structure a command; it shows the variables that must be supplied and the available options. A syntax line is a fragment of program code that shows how to use a particular routine; some syntax lines contain variables.

Convention	Meaning
boldface	In command lines and format lines: Indicates text (including punctuation) that you type verbatim from your keyboard. All DG/UX commands, pathnames, and names of files, directories, and manual pages also use this typeface.
`Typewriter`	Represents a system response on your screen. Syntax lines also use this font.
italic	In format lines: Represents variables for which you supply values; for example, the names of your directories and files, your username and password, and possible arguments to commands.
[ ]	In format lines: These brackets surround an optional argument. Don't type the brackets; they only set off what is optional. The brackets are in regular type and should not be confused with the boldface brackets shown below.
[ ]	In format lines: Indicates literal brackets that you should type. These brackets are in boldface type and should not be confused with the regular type brackets shown above.
...	In format lines and syntax lines: Means you can repeat the preceding argument as many times as desired.
$ and %	In command lines and other examples: Represent the system command prompt symbols used for the Bourne and C shells, respectively. Note that your

system might use different symbols for the command prompts.

↵ In command lines and other examples: Represents the New Line key, which is the name of the key used to generate a new line. (Note that on some keyboards this key might be called Enter or Return instead of New Line.) Throughout this manual, a space precedes the New Line symbol; this space is used only to improve readability—you can ignore it.

< > In command lines and other examples: Angle brackets distinguish a command sequence or a keystroke (such as **<Ctrl-D>**, **<Esc>**, and **<3dw>**) from surrounding text. Note that these angle brackets are in regular type and that you do not type them; there are, however, boldface versions of these symbols that you do type.

Some chapters give instructions that require you to use **sysadm**. We use a special convention to show a generic path that you follow through the menus. Consider the following example:

```
8  Software → 2  Package → 1  Install
```

You would follow the sample menu path to install a software package. Each text item (Software, Package, and Install) is a unique menu item. The arrow (→) symbolizes the traversal through the menus. Menu paths always begin from the **sysadm** Main Menu.

Finally, in examples we use:

This typeface to show your entry.
`This typeface to show file contents.`

Contacting Data General

Data General wants to assist you in any way it can to help you use its products. Please feel free to contact the company as outlined below.

Manuals

If you require additional manuals, contact your local Data General sales representative.

Telephone assistance

If you are unable to solve a problem using any manual you received with your system, free telephone assistance is available with your hardware warranty and with most Data General software service options. If you are within the United States or Canada, contact the Data General Customer Support Center (CSC) by calling 1–800–DG–HELPS. Lines are open from 8:00 a.m. to 5:00 p.m., your time, Monday through Friday. The center will put you in touch with a member of Data General's telephone assistance staff who can answer your questions.

For telephone assistance outside the United States or Canada, ask your Data General sales representative for the appropriate telephone number.

Joining our users group

Please consider joining the largest independent organization of Data General users, the North American Data General Users Group (NADGUG). In addition to making valuable contacts, members receive *FOCUS* monthly magazine, a conference discount, access to the Software Library and Electronic Bulletin Board, an annual Member Directory, Regional and Special Interest Groups, and much more. For more information about membership in the North American Data General Users Group, call 1–800–253–3902 or 1–508–443–3330.

End of Preface

Contents

Chapter 1 Getting Started

NetWare requirements 1-2
Environment 1-2
Uninterruptible power supplies 1-2
Where to go from here 1-3

Chapter 2 Installing NetWare on a New or Existing System

Installing NetWare for the first time 2-2
Creating NetWare virtual disks and file systems 2-3
Installing NetWare software 2-6
Rebooting the server 2-13
Installing NetWare on an existing system 2-14
Backing up existing file attributes and trustee rights 2-15
Rebooting the server 2-25
Restoring the file attributes and trustee rights 2-26
Configuring DG/UX printers on NetWare with pconfig 2-28
Where to go from here 2-32

Chapter 3 Router Installation and Management

Copying ROUTEGEN to diskette 3-1
Copying LAN drivers from server to diskette 3-2
Installing and generating router software 3-2
Managing routers 3-5

Chapter 4 Network File Services Setup

What you need 4-2
Planning the directory structure 4-3
Planning the system–created directories 4-5
Planning additional directories (optional) 4-6
Directory planning example 4-8
Planning the users and groups 4-10
Determining usernames 4-11
Planning hybrid users (optional) 4-11
Planning workgroups (optional) 4-12
Planning groups 4-13
Deciding which utility to use for user definition 4-14
Users and groups example 4-15
Deciding whether to install Accounting 4-17
Planning defaults for defining users 4-18
Planning the network security 4-32
Planning rights security for users and groups 4-33
Planning attribute security for directories and files 4-38
Planning the login scripts 4-43
Planning for login script conventions 4-44
Planning a system login script 4-45
Creating the directory structure 4-54
Installing DOS on the network 4-55
Creating directories 4-57
Loading application program files and setting file attributes 4-58
Flagging the principal executable file Execute Only 4-60
Copying any necessary files onto the workstation boot diskettes 4-64
Copying data files into directories 4-64
Using FLAG or FILER to assign file attribute security (optional) .. 4-64

Setting up the users with SYSCON 4-65
Installing the Accounting feature (optional) 4-65
Setting system defaults for users. 4-66
Creating groups 4-69
Assigning trustee rights. 4-70
Assigning trustee file rights 4-72
Creating users and setting up user accounts 4-74
Assigning password, station, and time restrictions to users 4-77
Creating a username directory for each user 4-82
Adding users to groups as members 4-85
Designating a workgroup manager (optional) 4-88
Designating user account managers (optional) 4-89
Creating the system login script 4-90
Creating users' login scripts 4-92
Creating hybrid users 4-94
Where to go from here 4-94

Appendix A Login Script Commands

(Executes a valid .COM or .EXE file.) A-7
Command format A-7
How to use # A-7
Example A-8
ATTACH A-9
Command format A-9
How to use ATTACH A-9
Example A-10
BREAK A-12
Command format A-12
How to use BREAK A-12
COMSPEC A-13
Command format A-13
How to use COMSPEC A-13
Examples A-13
DISPLAY A-15
Command format A-15
How to use DISPLAY A-15
Example A-15
DOS BREAK A-17
Command format A-17
How to use DOS BREAK A-17
DOS SET A-18
Command format A-18
How to use DOS SET A-18
Example 1 ..... A-18
Example 2 ..... A-19
Example 3 ..... A-19
Example 4 ..... A-20

DOS VERIFY A-21
Command format A-21
How to use DOS VERIFY A-21
DRIVE A-22
Command format A-22
How to use DRIVE A-22
Example A-22
EXIT A-23
Command format A-23
How to use EXIT A-23
Example 1 ..... A-24
Example 2 ..... A-24
Example 3 ..... A-24
Example 4 ..... A-24
FDISPLAY A-25
Command format A-25
How to use FDISPLAY A-25
Example A-25
FIRE PHASERS A-27
Command format A-27
How to use FIRE PHASERS A-27
Example 1 ..... A-27
Example 2 ..... A-27
GOTO A-28
Command format A-28
How to use GOTO A-28

IF...THEN...ELSE A-29
Command format A-29
How to use IF...THEN...ELSE A-29
Identifier variables A-29
ERROR_LEVEL A-30
NETWORK_ADDRESS A-31
[NOT] MEMBER OF "GROUP" A-31
P_STATION A-32
Command line parameters A-32
Relationships in conditionals A-34
Entering login script commands after THEN A-35
Single statement A-36
Block of commands A-36
INCLUDE A-37
Command format A-37
How to use INCLUDE A-37
Example 1 ..... A-37
Example 2 ..... A-38
MACHINE A-39
Command format A-39
How to use MACHINE A-39
MAP A-40
Command format A-40
Command options A-40
Variations of the MAP command A-41
MAP A-41
MAP drive:=directory A-41
MAP drive:=directory; drive:=directory A-41
MAP drive:=drive: A-42
MAP DISPLAY OFF A-42
MAP DISPLAY ON A-42
MAP ERRORS OFF A-42
MAP ERRORS ON A-42
MAP INSERT search drive:=directory A-42
MAP ROOT drive:=directory; drive:=drive A-43

How to use MAP A-43
Example 1 ..... A-45
Example 2 ..... A-45
Example 3 ..... A-45
Example 4 ..... A-45
Example 5 ..... A-46
PAUSE A-47
Command format A-47
How to use PAUSE A-47
PCCOMPATIBLE A-48
Command format A-48
How to use PCCOMPATIBLE A-48
REMARK A-49
Command format A-49
How to use REMARK A-49
Example A-49
SHIFT A-51
Command format A-51
How to use SHIFT A-51
WRITE A-54
Command format A-54
How to use WRITE A-54
Compound strings A-54
Example A-56
Sample system login scripts A-56
Example 1 ..... A-56
Example 2 ..... A-57
Example 3 ..... A-58
Sample user login script A-59
Example A-59

Appendix B Installation Worksheets

Appendix C Installing NetWare for AViiON Systems on a Trusted DG/UX System

Creating NetWare virtual disks and file systems C–3
Installing the software C–3
Installing Transport software on Trusted DG/UX C–4
Installing Services software on Trusted DG/UX C–9
Rebooting the server C–9
Finishing up C–10
Making all NetWare users hybrid users C–10
Using audible events features C–11
Where to go from here C–12

Appendix D Installing and Using High Availability Features with NetWare

High availability methods D–2
Multi–path LAN I/O D–2
Server failover D–2
How NetWare server failover works D–4
Installing NetWare with server failover D–6
Preparing to install NetWare with server failover D–7
Installing NetWare with server failover D–8
Modifying server failover with scripts D–25
Setting up NetWare to continue printing after failover D–27
Where to go from here D–28

1 Getting Started

This chapter gives a brief introduction to NetWare® for AViiON® Systems. It also includes general hardware requirements and tells you where to go from here to get your NetWare for AViiON System up and running.

As a *distributed, client / server* application, part of the NetWare for AViiON Systems software runs under DG/UX™ on an AViiON® series system (the server), and part runs under the MS–DOS® operating system (on a PC) or under OS/2 (on a Macintosh®) on each workstation (the clients). See the Release Notice for this product for the specific hardware and software requirements of NetWare for AViiON file server and workstations.

NetWare requirements

This section gives general NetWare network requirements. To protect the investment you have made in your file server, workstations, and attached peripherals, your installation site should meet certain physical requirements. Refer to the environmental specifications listed in the hardware manuals that shipped with your AViiON server for a description of these physical requirements.

Environment

Consult your Starting manual for your AViiON system's specific requirements in the following areas:

- Temperature/humidity
- Maximum altitude
- Minimum clearance
- Power source
- Power frequency
- Power requirements
- Power consumption

Uninterruptible power supplies

Protect file servers from power fluctuations with a regulating uninterruptible power supply (UPS). Besides protecting hardware from damage from power surges and voltage spikes, a UPS protects data held in RAM during a power failure.

We strongly recommend that you use UPS protection for network workstations and other peripherals. If this is not feasible, try to equip them with a power conditioning device. See *Concepts* for descriptions of these devices.

Where to go from here

For initial hardware setups:

- If you need to install your AViiON server, or a PC or Macintosh workstation, see the documentation that shipped with these computers.
- If you need to install cabling before installing NetWare on your AViiON server, see the documentation that shipped with your AViiON server and network boards.

With the initial hardware preparation completed, you are ready to upgrade or install NetWare for AViiON Systems on the server.

If you are a system administrator, you should read each chapter in this manual in sequential order. If a task is optional, the beginning of the chapter describing the task will indicate that it is optional. You can then skip sections as necessary.

If you are planning to customize the NetWare network or activate any advanced network features, we recommend that you do the following:

- Fill in the blank File Server installation Worksheets in Appendix B.
- Review the remaining installation worksheets in Appendix B and fill in the worksheets related to the feature or area you intend to customize or activate.

For installing NetWare for AViiON Systems for the first time *without* server failover:

- See section "Installing NetWare for AViiON Systems" in Chapter 2 to prepare your AViiON system and install the file server software.
- If you have DG/UX printers (configured with **sysadm**) that you want to configure on your NetWare system, see section "Configuring DG/UX Printers on NetWare with pconfig" in Chapter 2.
- If you have a router, see Chapter 3 "Router Installation and Management" to prepare it and to install the router software.
- See the Novell® NetWare manual(s) you received with your client software for instructions on setting up DOS, Macintosh, or OS/2 workstations.
- Continue with Chapter 4 "Network File Services Setup" to plan your network environment, create the directory structure, install applications, load files, define users, and set up NetWare security.
- See *Print Server* to set up your printing environment.

For installing NetWare for AViiON Systems on an existing NetWare system *without* server failover:

- Read "Getting Started" to ensure your working environment, power requirements, and working diskettes are ready.
- Read "Installing NetWare on an existing system" to install NetWare on a system running Revision 2.xx of NetWare for AViiON Systems and to upgrade your data's file system.
- If you have a router, see Chapter 3 "Router Installation and Management" to prepare it and to install the router software.
- See the Novell® NetWare manual(s) you received with your client software for instructions on setting up DOS, Macintosh, or OS/2 workstations.
- If you have DG/UX printers (configured with **sysadm**) that you want to configure on your NetWare system, see section "Configuring DG/UX Printers on NetWare with PConfig" in Chapter 2.
- See *Print Server* to set up your printing environment.

For installing NetWare for AViiON Systems *with* server failover on a new or existing system:

- Read "Getting Started" to ensure your working environment, power requirements, and working diskettes are ready.
- Read Appendix D and sections on failover in *Managing the DG/UX System* and *Achieving High Availability on AViiON Systems* before you install NetWare with server failover. Use procedures in Appendix D to install NetWare on a new or existing system with server failover.

- If you have a router, see Chapter 3 "Router Installation and Management" to prepare it and to install the router software.
- See the Novell® NetWare manual(s) you received with your client software for instructions on setting up DOS, Macintosh, or OS/2 workstations.
- Continue with Chapter 4 "Network File Services Setup" to plan your network environment, create the directory structure, install applications, load files, define users, and set up NetWare security.
- If you have DG/UX printers (configured with **sysadm**) that you want to configure on your NetWare system, see section "Configuring DG/UX Printers on NetWare with ponfig" in Chapter 2.
- See *Print Server* to set up your printing environment.

If you are a user who plans to install the NetWare for AViiON software on your workstation, you can proceed to Chapter 3. Before doing so, however, ask your Network system administrator whether you can install the software at this time. The administrator must perform the tasks in Chapters 2 and 4 before you install the software on your workstation.

End of Chapter

2 Installing NetWare on a New or Existing System

This chapter tells how to install NetWare for AViiON Systems on a new or existing system. Refer to the NetWare for AViiON Systems Transport and Services Release Notices for hardware and software prerequisites before you begin the installation.

This chapter describes the following procedures:

- Installing NetWare for the first time
- Installing NetWare on an existing NetWare System
- Configuring DG/UX printers on the NetWare network with **pconfig**.

NOTE: We recommend that you fill in the File Server Worksheet (in Appendix B) before you begin the installation if you plan to customize the network or activate any advanced network features. However, most users can set up the NetWare network without using a filled–in File Server Worksheet, by accepting defaults to prompts that appear during the installation.

For other types of NetWare installations, see:

- Appendix C: To install NetWare for AViiON Systems on a Trusted DG/UX system
- Appendix D: To install NetWare for AViiON Systems with server failover. (Trusted DG/UX does not support server failover)

The next section describes procedures for installing NetWare for the first time. If you have NetWare Revision 2.xx installed on your system, begin the installation with the section "Installing NetWare software on an existing system."

Installing NetWare for the first time

To install NetWare for AViiON Systems for the first time, first follow recommendations in Chapter 1. Then do the following tasks in order:

1. Create virtual disks and file systems for NetWare system files and user files.
2. Install the NetWare Transport software.
3. Optionally, install the NetWare Services software.
4. Reboot the AViiON server.

IMPORTANT: The system is case–sensitive, so you must type characters exactly as they appear in this manual.

The sections that follow explain how to do these tasks.

Creating NetWare virtual disks and file systems

Follow these steps.

IMPORTANT: If you plan to install the NetWare software with server failover, procedures in this section will include an additional requirement. See the section "Installing the Services software with server failover" in Appendix D for details on this requirement.

1. Log on as root. Make sure all users have logged off the system.
2. Take the system to run level 1. Type:

   init 1 ↵
3. Log on again as root.
4. Use **sysadm** to create virtual disks for NetWare. Type:

   asysadm ↵

   Follow the **sysadm** Main menu path:

   ```
   2  File System → 3  Local Filesys  →
   1  Create
   ```

5. Create and add the **usr/opt/netware** file system.

Use this information to answer the **sysadm** prompts:

```
Virtual Disk: [ ] usr_opt_netware
Mount Directory (optional): /usr/opt/netware
Blocks to Allocate: (1-530063) [1] 75000
```

Accept the defaults at the remaining prompts, as indicated below.

```
Virtual Disk: [ ] usr_opt_netware
Mkfs Options:
Mount Directory (optional): /usr/opt/netware
Exportable? [no]
Blocks to Allocate: (1-530063) [1] 75000
OK to perform operation? [yes]
```

... (The system pauses while creating the file system. Then the status message display continues.)

```
Virtual disk "usr_opt_netware" created.
Virtual disk "usr_opt_netware" made a volume.
Virtual disk usr_opt_netware created (7500 blocks).
File system created on virtual disk
/dev/dsk/usr_opt_netware.
File system added: /usr/opt/netware
File system mounted: /usr/opt/netware
```

6. If you are installing Services, create and add the **usr/netware** file system.

   The NetWare filing system consists of logical pieces called *volumes*. The **usr/netware** file system is the SYS volume, which is the initial NetWare system volume that you define in this step. You can define other volumes later.

   Note that 200,000 blocks equal 100 megabytes, which is the recommended default.

   Follow the **sysadm** Main menu path:

   ```
   2  File System → 3  Local Filesys
    → 1  Create
   ```

   Use this information to answer the **sysadm** prompts:

   ```
   Virtual Disk: [ ] usr_netware
   Mount Directory (optional): /usr/netware
   Blocks to Allocate: (1-530063) [1] 200000
   ```

   Accept the defaults at the remaining prompts, as indicated below.

   ```
   Virtual Disk: [ ] usr_netware
   Mkfs Options:
   Mount Directory (optional): /usr/netware
   Exportable? [no]
   Blocks to Allocate: (1-530063) [1] 200000
   OK to perform operation? [yes]
   ```

   ... (The system pauses while creating the file system. Then the status message display continues.)

   ```
   Virtual disk "usr_netware" created.
   Virtual disk "usr_netware" made a volume.
   Virtual disk usr_netware created (200000 blocks).
   File system created on virtual disk
   /dev/dsk/usr_netware.
   File system added: /usr/netware
   File system mounted: /usr/netware
   ```

7. Exit **sysadm**.

Procedures for creating NetWare virtual disks and file systems are now finished. Continue the installation with the next section.

Installing NetWare software

This section describes how to install the Transport software, and optionally, the Services software.

The NetWare software consists of two packages: Transport and Services. You must install the Transport package. You can optionally install the Services package for NetWare services such as printing and filing services. With the Transport package alone, the server can provide client users access to other NetWare servers on the network.

IMPORTANT: If you plan to install the Transport software with server failover, do *not* use the procedures in this section. Instead, use procedures in the section "Installing the Transport software with server failover" in Appendix D.

If you are installing NetWare for AViiON Systems on an existing NetWare Revision 2.xx system, use the installation procedures in the section "Installing NetWare software on an existing system" instead of procedures in this section.

If you are not familiar with procedures for installing software packages in DG/UX, refer to *Installing the DG/UX™ System* for details.

Follow these steps to install the NetWare software.

1. Make sure you are logged on as root, and that all other users have logged off the system.

2. Take the system to run level 1. Type:

   init 1 ↵

3. Log on again as root.

Continue the installation with the next section.

Installing the Transport software

Follow these steps.

1. Insert the NetWare Transport release media into the appropriate drive or device.

2. Use **sysadm** to install the Transport package. Type:

   asysadm installpackage ↵

3. Accept the defaults as indicated below.

   We recommend that you do not list file names as this slows down the load.

```
Release Medium: [/dev/rmt/0]
Is /dev/rmt/0 ready? [yes]
NetWare 3.11/Transport of mm/dd/yy from Data General
Corporation
Package name(s): [all]
List file names while loading? [no]
OK to perform operation? [yes]

Loading NetWare 3.11/Transport of mm/dd/yy from Data
General Corporation.

Positioning the tape to load: nw_tran:prep .....

Preparing to load the packages...

Loading package nw_tran ....
Package nw_tran has been loaded.
```

```
Package load is finished.
The selected packages have been loaded.
Setting up nw_tran in usr.
Installing NetWare 3.11/Transport for AViiON Systems.
  The group 'netware' must be created.
  Group ID? [690]

  The User 'netware' must be created.

  User ID? [690]
.........

Package nw_tran has been successfully set up in usr.
Setting up nw_tran in MY_HOST root.
..
```

4. Answer the **sysadm** prompts and accept the defaults at the remaining prompts, as indicated below. (For **xxxxxxxx**, type your choice or accept the default.) Your answers will look similar to the following example.

```
Most of NetWare can be configured automatically, but
for a couple of items, such as server name, some input
is required.
NVT Host Name?: [acme] acme
Probing the network ....
Internal Network Number?: [80ddefe6] xxxxxxxx
Probing the network....
Changing llc_devices_ARG in /etc/dgux.params file
```

5. Use this information to answer the **sysadm** prompts on choosing the system name, and optionally, installing server failover:

```
System Name?: [acme] acme
Install this NetWare server with Failover
support? [N]? N
```

CAUTION: The remaining screen display in this section assumes you answered **N** *at the prompt* `Install this NetWare server with Failover support?`. *If you plan to answer* **Y** *at this prompt, you must use the procedures in Appendix D for this step, and the remaining Transport installation steps. You must also read adapter failover sections in Managing the DG/UX System and Achieving High Availability on AViiON Systems for precautions and pre-installation procedures.*

Accept the defaults at the remaining prompts, as indicated below.

```
The NetWare transport needs to add items to the system
build files in order to complete the installation.
This step will verify that these items are properly
added before attempting to build the system.

System Name?: [acme] acme
Install this NetWare server with Failover
   support? [N] N
Configuring system....
Building kernel....
```

... (The system pauses while building the kernel. Then the status message display continues.)

```
Successfully built dgux.acme.
Linked /dgux. You must reboot in order for this kernel
to take effect. Installation of NetWare 3.11/Transport
is complete. Package nw_tran has been successfully set
up in MY_HOST root. Package setup for nw_tran is
complete.
```

Procedures for installing the Transport software are now finished. If you want to install Services software, continue the

installation with the next section. Otherwise, continue installation procedures in the section "Rebooting the Server."

Installing the Services software

IMPORTANT: If you plan to install the Services software with server failover, do *not* use the procedures in this section. Instead, use procedures in the Appendix D section "Installing the Services software with server failover."

Follow these steps.

1. Remove the Transport media and insert the Services media.

2. From the Package menu, choose:

   ```
   1  Install
   ```

   Accept the defaults for the prompts, as indicated below.

   We recommend that you do not list file names as this slows down the load.

   ```
   Release Medium: [/dev/rmt/0]
   Is /dev/rmt/0 ready? [yes]
   NetWare 3.11/Services of mm/dd/yy from Data General
   Corporation
   Package Name(s): [all]
   List file names while loading? [no]
   OK to perform operation? [yes]
   Loading NetWare 3.11/Services of mm/dd/yy from Data
   General Corporation [*]

   Positioning the tape to load: nw_serv:prep . . . .

   Preparing to load the packages ...

   Loading package nw_serv ....
   ```

... (The system pauses while loading the Services software. Then the status message display continues.)

```
Package nw_serv has been loaded.
Package load is finished.
The selected packages have been loaded.
Setting up nw_serv in usr.

     Removing obsolete files from previous releases,
     if present .... Done
     Setting /srv/release/PRIMARY/usr/opt/netware
     ownerships .... Done
     Setting /srv/release/PRIMARY/usr/netware
     ownerships .... Done
```

Then the following messages appear.

```
Package nw_serv has been successfully set up in usr.
Setting up nw_serv in MY_HOST root

Setting default hybrid user and group id values ....
  Done
```

3. Specify your File Server name, License Validation Key, and whether you want to install NetWare with server failover.

   Use the following information to answer the **sysadm** prompts:

   `File Server Name [acme]` **acme**

   The File Server Name is the name of the AViiON server on which you are installing the software. If the name of your system does not appear as the default, type the correct hostname. We use "acme" in our example.

   `NetWare 3.11 License Validation Key [abcde12345]` **xxxxxxxxxx**

   The License Validation Key is on the key sheet that ships with the Services license. The key is a

ten–character alphanumeric code; it is case–sensitive, so type it exactly as it appears on the license key sheet. We use abcde12345 in our example.

NOTE: If you have a five–user license, accept the default at the License Validation Key prompt.

```
Install this NetWare server with failover
support? [N]? N
```

IMPORTANT: The remaining screen display in this section assumes you answered **N** at the prompt `Install this NetWare server with failover support? [N]?` If you plan to answer **Y** at this prompt, you must use the procedures in Appendix D for this step, and the remaining Services installation steps.

4. Exit **sysadm**.

IMPORTANT: If you are installing NetWare in an existing NetWare environment, we recommend that you use SCONSOLE to review the following Transport configurations to be sure that they are correctly set:

- The internal network number
- The network assignments

Procedures for installing the Services software are now finished. Continue the installation with the next section.

Rebooting the server

Follow these steps.

1. Type:

   shutdown -g0 -y ↵

   halt -q ↵

2. Reboot the system and return to init level 3.

Procedures for installing NetWare for AViiON System software are now finished. Now each time you boot the AViiON server, the Transport and Services software (if installed) begin running automatically.

NOTE: The Transport starts at DG/UX init level 2; the Services start at DG/UX init level 3.

If NetWare is running when the server is shut down, the Transport and Services automatically shut down. You can also start and stop NetWare by using the SCONSOLE utility, as explained in *System Administration*.

If you have DG/UX printers (configured with **sysadm**) that you want to configure in your NetWare network, see the section "Configuring DG/UX printers on NetWare with **pconfig**." Otherwise, see the section "Where to go from here" at the end of this chapter.

Installing NetWare on an existing system

To upgrade NetWare for AViiON Systems from Revision 2.xx, you must install NetWare 3.11 for AViiON 3.00 software over your existing revision 2.xx or later NetWare software. Follow recommendations in Chapter 1 before you begin installing NetWare on an existing system.

IMPORTANT: If you are running NetWare Revision 1.xx software, you must upgrade to Revision 2.xx, before following procedures in this section. See the NetWare for AViiON Systems Transport and Services Release Notices for these procedures.

To install NetWare on an existing system, do the following tasks in order:

1. Optionally, run **nwbackup** to back up your inodes files. You *must* run **nwbackup** either before or during Services installation. We recommend that you run **nwbackup** before the installation.
2. Install the NetWare Transport software.
3. Optionally, install the NetWare Services software.
4. Reboot DG/UX and the NetWare network.
5. Run the **nwrestore** utility to restore the backup file system.
6. Optionally, configure DG/UX printers (that were configured with **sysadm**) on a NetWare network with **pconfig**.

The sections that follow explain how to do these tasks.

IMPORTANT: The system is case–sensitive, so you must type characters exactly as they appear in this manual.

Backing up existing file attributes and trustee rights

This section tells how to run **nwbackup** before installing Services software on existing NetWare systems. We recommend that you run **nwbackup** before installing NetWare as the backup process can take considerable time.

Compared with pre–3.00 revisions, NetWare 3.11 for AViiON Systems 3.00 inodes files are much smaller, and the format uses only 20 – 40% as much space. Because of these changes, you must do the following tasks to convert your existing inodes files:

1. Run **nwbackup** before or during Services software installation to back up existing (pre–3.00 revision) inodes information and trustee rights. This section tells how to run **nwbackup** before installing Services software.

2. Install NetWare software over your existing NetWare software.

3. Run **nwrestore** to restore the back–up information, as described in the section "Restoring the back–up file attributes and trustee rights."

CAUTION: NetWare 3.11 for AViiON Systems 3.00 deletes existing earlier revisions of file attributes and trustee rights during the Services installation.
*If you fail to run **nwbackup** before or during a Services installation on an existing system, you will not have a copy of file attributes and trustee rights to restore after you finish installing NetWare.*

Follow these steps to run **nwbackup**.

1. Verify that NetWare Services software is up and has finished initializing. You can do so by running **slist**.

2. Move to the appropriate directory. Type:

   cd /usr/opt/netware/bin ↵

3. Run **nwbackup**. Type the name of the utility followed by the pathname to the directory designated to store the back–up information. (Make sure this directory has enough space to hold the information.) Type:

   ./nwbackup /usr/opt/netware ↵

4. Enter the supervisor's password. Press **<Enter>** if no supervisor's password exists.

NOTE: The backup process can take considerable time.

The system displays the following messages (and continually updates the numbers during the backup).

```
Starting the Backup.
Backing up the SYS volume.
       272 Done.
       264 Files were scanned.
         8 Directories were scanned.*
Backing up trustee info.
          3 Done.
End of Backup.
```

For more information on **nwbackup** and **nwrestore**, see *Utilities*.

Installing Transport over existing software

Follow these steps.

IMPORTANT: If you plan to install the Transport software with server failover, do *not* use the procedures in this section. Instead, use procedures in the Appendix D section "Installing the Transport software with server failover."

1. Make sure that NetWare is up and running.
2. Take the system to run level 3. Type:

   init 3 ↵
3. Log on again as root.
4. Insert the NetWare Transport release media into the appropriate drive or device.
5. Use **sysadm** to install the Transport software. Type:

   asysadm installpackage ↵

6. Accept the defaults for the **sysadm** prompts as indicated below.

   We recommend that you do not list file names as this slows down the load.

```
Release Medium: [/dev/rmt/0]
Is /dev/rmt/0 ready? [yes]
NetWare 3.11/Transport of mm/dd/yy from Data General
Corporation

Package Name(s): [all]
List file names while loading? [no]
OK to perform operation? [yes]
Loading NetWare 3.11/Transport of mm/dd/yy from Data
General Corporation
Positioning the tape to load: nw_tran:prep ....

Preparing to load the packages ....

   This installation of NetWare is Rev 2.x.

Loading package nw_tran ....
Package nw_tran has been loaded.
Package load is finished.
The selected packages have been loaded.
Setting up nw_tran in usr.
Installing NetWare 3.11/Transport for AViiON Systems...
   Group netware already installed
   User netware already installed
.............

Package nw_tran has been successfully set up in usr.
Setting up nw_tran in MY_HOST root.
```

7. Use this information to answer the **sysadm** prompts:

```
System Name?: [acme] acme
Install this NetWare server with Failover
support? [N] N
```

CAUTION: The remaining screen display in this section assumes you answered **N** *at the prompt* `Install this NetWare server with Failover support?`. *If you plan to answer* **Y** *at this prompt, you must use the procedures in Appendix D for this step, and the remaining Transport installation steps. You must also read Appendix D and adapter failover sections in Managing the DG/UX System and Achieving High Availability on AViiON Systems for precautions and pre-installation procedures.*

Accept the defaults at the remaining prompts, as indicated below.

```
   The NetWare transport needs to add items to the
   system build files in order to complete the
   installation.  This step will verify that these
   items are properly added before attempting to build
   the system.

   System Name?: [acme] acme
   Install this NetWare server with Failover support?
    [N]? N
Configuring system...
Building kernel...
```

... (The system pauses while building the kernel. Then the status message display continues.)

```
Successfully built dgux.acme.
Linked /dgux. You must reboot in order for this kernel
to take effect.
Installation of NetWare 3.11/Transport is complete.
Package nw_tran has been successfully set up in MY_HOST
root.
Package setup for nw_tran is complete.
```

Procedures for installing the Transport software on an existing NetWare system are now finished. Continue the installation with the next section.

Installing Services over existing software

If you are installing Services software, follow these steps. If you are not installing Services software, skip to the next section to continue the installation procedures.

IMPORTANT: If you plan to install the Services software with server failover, do *not* use the procedures in this section. Instead, use procedures in the section "Installing the Services software with server failover" in Appendix D.

1. Remove the Transport media and and insert the Services media into the appropriate drive or device.

2. From the **sysadm** Packages Menu, follow the path:

```
1  Install
```

3. Accept the defaults at the following prompts as indicated below.

   We recommend that you do not display file names as this slows down the load.

```
Release Medium: [/dev/rmt/0]
Is /dev/rmt/0 ready? [yes]
NetWare 3.11/Services of mm/dd/yy from Data General
Corporation [*].
Package Name(s): [all]
List file names while loading? [no]
OK to perform operation? [yes]
Loading NetWare 3.11/Services of mm/dd/yy from Data
General Corporation.

Positioning the tape to load: nw_serv:prep ....
```

```
Preparing to load the packages ...

   This installation of NetWare is Rev 2.x.

An upgrade of your 2.x system to 3.x is recommended.
This upgrade procedure includes saving the NetWare
specific information associated with files on your
volumes. Additionally, the trustee database is saved.
This process is done by using the nwbackup utility.

You have the option of skipping this step. You may skip
the nwbackup if you have already run the backup
program, or if you do not wish to save your NetWare
specific information or your trustee database.
```

4. Use this information to answer the **sysadm** prompts:

```
Proceed with the nwbackup? [Yes]
```

CAUTION: NetWare 3.11 for AViiON Systems 3.00 deletes existing inodes files of earlier revisions during the Services installation.
*If you have not already run **nwbackup**, you must answer **Y** at this prompt to run **nwbackup** now. Otherwise, you will not have a copy of your current file attributes and trustee rights database to restore after you finish the installation.*

Answer **N** if you already ran **nwbackup**, or if you do not want to save your current file attributes and trustee rights. Then the system displays the message
`The nwbackup process has been skipped.`

If you answer **Y**, the system prompts you to enter a path for the backup files and the supervisors password.
In our example, we answer **Y**.

```
Path for NetWare Backup Files to be placed
[/srv/release/PRIMARY/usr/opt/netware]
```
/srv/release/PRIMARY/usr/opt/netware

Make sure you specify a path to a location on a file system with enough free space to hold your file attributes

and trustee rights database. Depending on the size of your current NetWare files, **nwbackup** can take an hour or more to back up information.

```
Enter SUPERVISOR's password: xxxxxx
```

Accept the defaults at the remaining prompts as indicated below.

```
Proceed with the nwbackup? [Yes]
Proceeding with the upgrade...

Path for NetWare Backup Files to be placed
[/srv/release/PRIMARY/usr/opt/netware]
    /srv/release/PRIMARY/usr/opt/netware

   Estimating the number of files on your NetWare
   volume(s)...

   Estimated number of files on NetWare volume(s): 5779

User SUPERVISOR logging into server acme...
Enter SUPERVISOR's password: xxxxxx
```

... (The system pauses to do the backup. Depending on the size of your file system, the backup can take up to an hour or longer. Then the status message display continues.)

```
Starting the Backup.
Backing up the SYS volume.
5778 Done.
5428 Files were scanned.
350 Directories were scanned.*
Saving trustee info.
11 Done.
```

... (The system continually updates the numbers in the above prompts during the backup process. Then the status message display continues.)

```
End of Backup.
```

```
Stopping NetWare...
NWInform: NetWare (acme) shutdown started.
NWInform: ACME waiting for clients to respond.
NWInform: NetWare ACME down.

   Removing the inodes..

   Removing the trustee database...

   Loading package nw_serv .....
```

... (The system pauses while loading the Services software. Then the status message display continues.)

```
Package nw_serv has been loaded.
Package load is finished.
The selected packages have been loaded.
Setting up nw_serv in usr.
   Removing obsolete files from previous releases,
   if present ... Done

   Setting /srv/release/PRIMARY/usr/opt/netware
   ownerships .... Done
   Setting /srv/release/PRIMARY/usr/netware ownerships
   .. Done

   Setting default hybrid user and group id values
   ...Done

*** NOTE ***
This installation is an upgrade from 2.x to 3.x.
You must reboot the system with the new kernel. Bring
the machine to level 3 and wait for the NetWare inodes
to rebuild. You must run the NetWare Restore program
manually.

Check release notice for more details...
```

5. Answer the server failover prompt.

```
Install this NetWare server with Failover
support? [N] N
```

IMPORTANT: If you plan to answer **Y** at this prompt, you must use the procedures in Appendix D for this step, and the remaining Service installation steps.

Then the system displays messages indicating that the Service package has successfully loaded.

```
Package nw_serv has been successfully set up in MY_HOST
root.
Package setup for nw_serv is complete.
```

6. Exit **sysadm**.

Procedures for installing the Services software on an existing NetWare system are now finished. Continue the installation with the next section.

Rebooting the server

Follow these steps.

1. Move to the root directory. Type:

   cd / ↵

2. Type:

   shutdown -g0 -y ↵

   halt -q ↵

3. Reboot the system and return to init level 3.

NOTE: If you are upgrading from Revision 2.xx, the system takes longer than usual to reboot the first time you start NetWare, as it must rebuild the inodes files.

Continue the installation with the next section.

Restoring the file attributes and trustee rights

Follow these steps.

1. Verify that NetWare Services software is up and has finished initializing. You can do so, by running **slist**.

2. Move to the appropriate directory. Type:

   cd /usr/opt/netware/bin ↵

3. Run **nwrestore**. Type the name of the utility followed by the pathname to the directory storing the back–up information:

   ./nwrestore /usr/opt/netware ↵

4. Enter the supervisor's password. Press **<Enter>** if no supervisor's password exists.

NOTE: The restore process can take considerable time.

The system displays the following messages (and continually updates the numbers during the restore process).

```
Starting the Restore.
       272 Done.
       264 Files were restored.
         8 Directories were restored.*
Restoring trustee info.
          3 Done.
End of Restore.
```

For more information on **nwbackup** and **nwrestore**, see *Utilities*.

Procedures for installing NetWare on an existing NetWare Revision 2.xx system are now finished. Now each time you boot

the AViiON server, the Transport and Services (if installed) software automatically begin running.

If you have DG/UX printers (configured with **sysadm**) that you want to configure in your NetWare network, see the section "Configuring DG/UX Printers on NetWare with **pconfig**." Otherwise, see the section "Where to go from here" at the end of this chapter.

Configuring DG/UX printers on NetWare with pconfig

This section describes how to configure DG/UX printers on the NetWare network with the **pconfig** utility.

Beginning with NetWare Revision 2.10, we include **pconfig**, a simple procedure that lets you configure printers on the NetWare network after you install NetWare. **pconfig** configures *only* DG/UX printers that were configured in DG/UX with **sysadm**.

You can use **pconfig** to get your DG/UX printers up and running on the NetWare network. Later, you can use other procedures to configure other printers (such as remote printers) modify print queues, or customize printers. To perform these and other advanced printer procedures, see *Print Server* and the "SCONSOLE Utility" chapter in *System Administration*.

IMPORTANT: The system is case–sensitive, so you must type characters exactly as they appear in this manual.

Follow these steps.

1. Log on as root.
2. Make sure the system is at init level 3 and that the network services are running.
3. Change to the correct directory. Type:

   cd /bin/netware ↵

4. Before you configure printers with **pconfig**, determine that printers exist in DG/UX and that they have been configured with **sysadm**. Type:

lpstat -p ↵

The system displays a list of DG/UX printers configured with **sysadm**. If the printer you want to configure on NetWare is not on this list, you must configure that printer on your DG/UX system with **sysadm** before continuing with **pconfig**. See *Managing the DG/UX System* for details on configuring printers in DG/UX.

5. Run the **pconfig** utility. Type:

   ./pconfig ↵

   The system displays the name of the server you are logged onto, and prompts you for the supervisor's password. As an example, the system displays:

```
User SUPERVISOR logging into server acme
Enter SUPERVISOR'S password:__
```

6. Type the supervisor's password (or press Enter if no supervisor's password exists).

   The system display tells you that a print server exists, or that it is creating a print server. As an example, the system displays:

```
NetWare 3.11 for AViiON Systems

Simplified Printer Configuration Utility (pconfig)

Copyright Data General Corporation 1994
All Rights Reserved

User SUPERVISOR logging into server acme...
Enter SUPERVISOR's password:

Creating a Print Server with the name acme
Creation completed.
Extracting printer information...please wait

List of print queues defined in DG/UX:
```

```
1: PS1:
2: PS2
3: LP1
4: WPUSERS
5: PAYROLL
6: SPREADSHEET

List of printers defined in NetWare:

Enter printer to add to NetWare:  ?
Respond with one of the following:
   - a number from 1 to the number of Unix printers
listed
   - the name of a Unix printer
   - the word 'all' (with no quotation marks) for all
printers
   - the word 'quit' (no quotes) to exit

Enter printer to add to NetWare: ___
```

The screen display in the above example lists the printers you can configure on NetWare with **pconfig**. You can configure any or all of the printers on the list.

7. Enter **all** to configure all printers on the list, or enter the name or number to configure one printer.

   In our example, to configure all printers on the list, you would enter:

   ```
   Enter printer to add to NetWare: all ↵
   ```

   To configure one printer on the list, enter that printer's number:

   ```
   Enter printer to add to NetWare: 1 ↵
   ```

Or, to configure one printer, you can also enter that printer's name:

```
Enter printer to add to NetWare: PS1 ↵
```

In our example, if you enter **1** or **PS1**, the system responds by displaying the following:

```
List of print queues defined in DG/UX:
1: PS1   Fully configured in NetWare
2: PS2
3: LP1
4: WPUSERS
5: PAYROLL
6: SPREADSHEET

List of printers defined in NetWare:

1: PS1

Enter printer to add to NetWare:__
```

8. To configure more printers, repeat Step 7. When you are finished, type **quit**, as shown in our example:

```
Enter printer to add to NetWare: quit ↵
```

The system displays the following:

```
The file /usr/opt/netware/bin/psinit has been updated
so that Print Services will automatically begin the
next time your system is brought up. to init level 3.
```

pconfig procedures for configuring printers to NetWare are now finished.

Where to go from here

Use this information to determine where to continue the NetWare network installation process.

If you need to	See
Install a DOS Workstation	*NetWare Requester for DOS*
Install an OS/2 workstation	*NetWare Requester for OS/2*
Install a MacIntosh workstation	*NetWare for MacIntosh Installation and Maintenance*
Install a router (bridge)	Chapter 3 – "Router Installation Management"
Install cabling	Installation supplements or documentation that ships with your network boards
Set up diskless workstations	*NetWare Requester for DOS*
Create users, directories, and network security	Chapter 4 – "Network File Services Setup"

End of Chapter

3 Router Installation and Management

This chapter gives instructions for the following tasks:

- Copying the ROUTEGEN program from the NetWare directory structure to a formatted diskette
- Copying the LAN drivers from the NetWare directory structure to a formatted diskette
- Installing and generating router software
- Setting up and managing a dedicated or nondedicated router

The sections that follow explain how to do these tasks.

Copying ROUTEGEN to diskette

The ROUTEGEN program is located in the SYS:PUBLIC directory.

Follow these steps.

1. Boot DOS and NetWare on a workstation and log in to the server as SUPERVISOR. See the NetWare workstation for DOS manual that comes with your client software.
2. Remove the diskette and insert a blank formatted diskette.
3. Copy the ROUTEGEN files to the diskette. Type:

   CD \PUBLIC\ROUTEGEN ↵
   COPY *.* A: ↵

4. Label the diskette *ROUTEGEN*.

   LABEL A:ROUTEGEN

Continue procedures for router installation in the next section.

Copying LAN drivers from server to diskette

Follow these steps.

1. Boot DOS and NetWare on a workstation and log in to the server as SUPERVISOR.

   See the NetWare workstation for DOS manual that comes with your client software.

2. Remove the diskette and insert a blank formatted diskette.

3. Copy files from LAN_DRV to diskette. Type:

   CD \PUBLIC\LAN_DRV_.001 ↵

   COPY *.* A: ↵

4. Label the diskette LAN_DRV_001.
   LABEL A:LAN_DRV_001

Continue procedures for router installation in the next section.

Installing and generating router software

The ROUTEGEN program generates a router (previously called a bridge). Routers transfer packets between networks that use different communication protocols, using the most efficient route.

Follow these steps to install a NetWare router after you have completed your operating system installation.

1. Log on and become root. Make sure all users have logged off the system.

2. Set up the LAN driver board. Follow the instructions that accompany the board.

3. Set the LAN board configuration option. Check for conflicts with other installed LAN boards.

4. Boot the workstation that you want to use as the router. Use a DOS diskette (version 3.0 or above) to boot the workstation.

5. Run ROUTEGEN. Insert the *ROUTEGEN* diskette into drive A and type

   ROUTEGEN ↵

   Several messages appear. Press <**Enter**> again to continue.

6. Enter the operating system mode.

   The router must be either dedicated or nondedicated. See *Concepts* for a description of these options. If you select nondedicated, enter a network address for the router.

7. Enter the number of communication buffers.

   The default is 150. You can use any number from 40 to 1000, but we recommend that you use the default setting.

8. Press <**Enter**> to accept the default setting, or type in the new number and press <**Enter**>.

9. Select a driver. Press <**Enter**> to see a list of available drivers. Select the driver you are using from the list. If it does not appear, complete the following steps:

   a. Press <**Insert**>.

   b. Insert the LAN_DRV_??? diskette (available from the manufacturer) into drive A and press <**Enter**>.

   c. Scroll to the driver you want, and then press <**Enter**>.

10. Select the router configuration option.

    The default configuration is recommended. Most boards are set at the factory to Option 0.

11. Repeat Steps 4 through 8 to select drivers and configurations for other network boards in your system.

    The maximum number of boards you can have in your system is four. If you are using a Token–Ring system, the maximum is two.

12. Check for configuration option conflicts.

13. Press <**F10**> to generate the router software.

    The system automatically links and configures the router operating system. When the process is complete, a message appears, indicating that ROUTEGEN has created the router.

See the next section for procedures on setting up and managing routers.

Managing routers

This section explains how to set up routers on a network after the router software has been installed and generated. It also explains how to boot dedicated and nondedicated routers.

Before setting up routers using procedures in this section, you should have installed the network hardware and software and installed and generated the router software, as discussed in the previous section.

Follow these steps to set up routers.

1. Create a router boot disk. After running ROUTEGEN, you are ready to create a boot disk that boots the router by doing either of the following:

   For a hard disk — Prepare the disk to boot with DOS according to the manufacturer's instructions.

   For a floppy diskette — Format a blank diskette using the DOS 3.*x* or 4.*x* FORMAT command and the /s parameter.

   The boot disk can be used for either a dedicated or nondedicated router.

2. Create a boot disk for a dedicated router as follows:

   a. Copy the ROUTER.EXE file to the boot disk (either floppy diskette or hard disk).

   b. Create an AUTOEXEC.BAT file on the boot disk using a text editor. To start the router, the batch file should have the following line:

3. Create a boot disk for a nondedicated router as follows:

   a. Copy the ROUTER.EXE file to the boot disk (either floppy diskette or hard disk).

   b. Create a CONFIG.SYS file on the boot disk with the following lines:

      FILES=20
      BUFFERS=20

   c. Create an AUTOEXEC.BAT file on the boot disk using a text editor. To start the router, the batch file should have the following lines:

      ROUTER
      NETX
      F:
      LOGIN

      (Replace NETX with NETX, EMSNETX, XMSNETX, or BNETX, depending upon the type of shell you want to use. These shells are described in *Concepts*.)

4. Boot the router workstation from the hard disk or the floppy diskette prepared in Step 1.

   When the router software is loaded, a message similar to the following appears:

   ```
   NetWare Real Mode Internetwork Router

   Initializing LAN A
   :
   ```

   If the router is dedicated, the console prompt (:) appears, indicating that the router is running.

   If the router is nondedicated, the router and the workstation files are loaded, and then you are prompted for a login name and password.

5. Load VAPs.

   If you need to load any VAPs, do so now. You may also need to create a ROUTER.CFG file. Refer to NetWare v2.*x* or NetWare for Macintosh documentation for more information on these.

Procedures for setting up and managing routers and finished.

End of Chapter

4 Network File Services Setup

This chapter gives the guidelines for planning and creating file services in your network environment.

Planning and creating your network environment involves the following tasks:

- Planning the directory structure
- Planning the users and groups
- Planning network security
- Planning login scripts
- Creating the directory structure
- Setting up the users with SYSCON
- Creating hybrid users

We suggest that your initial setup be simple. Your network will evolve as you find the most appropriate solutions for your needs.

What you need

To plan and create your network environment, you need a workstation where you are logged in as SUPERVISOR to create directories and users. You also need to copy and fill in the following worksheets (found in Appendix B):

- Directories Worksheet
- Users Worksheet
- Group Worksheet
- User Defaults Worksheet
- Trustee Directory Security Worksheet
- Trustee File Security Worksheet
- Login Scripts Worksheet

Record the planning decisions you make on the appropriate worksheets. The completed worksheets are your guide in creating your directory structure, setting up users, and providing appropriate NetWare security.

Planning the directory structure

Use the "Directory Structure" portion of the Directories Worksheet as you complete this section.

Planning the directory structure involves the following tasks:

- Planning the system–created directories
- Planning additional directories

The four directories already listed on the worksheet, LOGIN, MAIL, SYSTEM, and PUBLIC, are created automatically during network installation.

The NetWare directory structure created by installation is within NetWare volumes; these volumes are placed within the DG/UX directory tree and are not at the root level as seen on the server. For example, the LOGIN, MAIL, SYSTEM, and PUBLIC directories are created inside the SYS volume by the installation process; the SYS volume is at the root level as far as NetWare is concerned, but is below the root level as seen by the AViiON server.

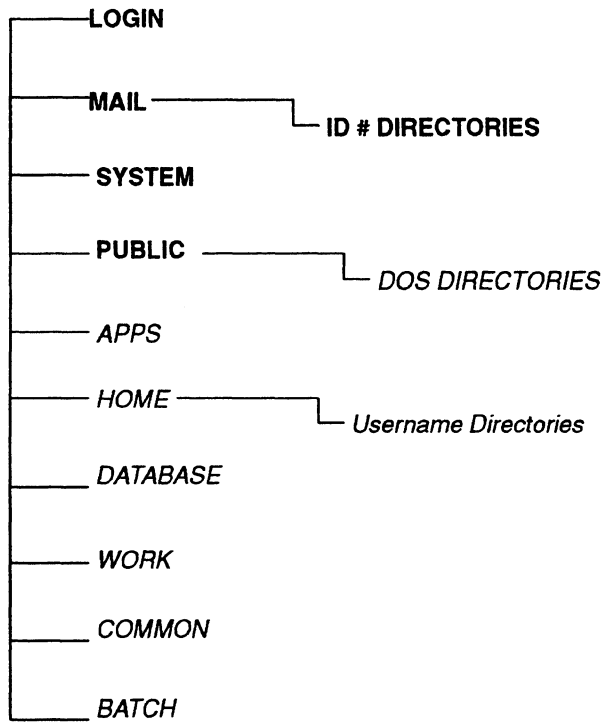
You can use SCONSOLE to create additional NetWare volumes in the AViiON server's DG/UX directory structure, then use other utilities to create directories inside those volumes. See *System Administration* for more information about creating the volumes in SCONSOLE. See **Directory structure (host)** and **Hybrid user** in *Concepts* for more information about the hybrid directory structure and hybrid users.

As network supervisor, you must create additional directories. Some directories, such as DOS directories, are essential. Others are optional, and you must decide whether they are appropriate for your needs. Directory names must conform to DOS naming conventions.

For more information and examples, see **Directory structure** in *Concepts*.

Planning the directory structure is easier when you use a diagram similar to the one following. In addition to the four system–created directories, the tree structure shows directories (in italics) that do not exist unless they are created. The directory structure illustrated below explains the purpose of each directory.

Directory Structure



Planning the system–created directories

The system automatically creates the directories listed in the following table. The appropriate files are copied to them during installation.

System–created directories

Directory	Explanation
SYS:LOGIN	This directory contains the programs necessary for logging in.
SYS:MAIL	This directory is used by mail programs that are compatible with NetWare. The directory also contains a subdirectory for each user in which the user login script and print job configurations are stored. The user subdirectories are created automatically when you create user login scripts and print job configurations.
SYS:SYSTEM	This directory contains operating system files as well as NetWare utilities and programs reserved for the network supervisor.
SYS:PUBLIC	This directory is for general access and contains NetWare utilities and programs for regular network users.

Planning additional directories (optional)

Decide which of the types of directories listed in table below fit your needs.

Additional directories

Directory Type	Explanation
DOS	To store DOS program files, plan one or more DOS directories. The number of DOS directories you create depends on the number of workstation brands and DOS versions on your network. See DOS directories in *Concepts* for guidelines and examples.
Application	To store application program files, check the documentation that accompanies the application. Typically, you will plan a directory for each application and other directories to keep the data files. If you have two or more volumes, install your applications on a volume other than the one the data files are on. You can simplify your daily backups by backing up only the data volume. You can still install an application that must be installed at the root directory level in a subdirectory because you can map a search drive to a fake root. See **MAP** in *Utilities*.
Username	To provide personal work space for users, plan a parent directory for username subdirectories and private username directories for all users.

Additional directories

Directory Type	Explanation
Work (data)	If you prefer to have users work in group work space or move completed work from their personal work space to a work directory, plan a separate directory for each major project. If you have two or more volumes, install your work directories on a volume other than the one the application files are on. You can simplify your daily backups by backing up only the work directories on the data volume.
Common or shareable	If you want a directory to serve as a transfer point for copying files to and from other directories (without having to consider rights), plan a directory for that purpose.
Batch file	If you do not want to store batch files in a public access directory, plan a directory for that purpose. You can use file trustee assignments and file attributes to adjust security.

When you have decided on the kinds of directories you want and how you want to organize them in a directory structure, record the directory names on the Directories Worksheet. (You may want to sketch a tree structure first to help you visualize the directories.) You complete the rest of this worksheet when you plan security for your directories and files.

Directory planning example

The file server acme has one volume. The network has both IBM and COMPAQ workstations. The IBM workstations are running three versions of DOS, and the COMPAQs are running one version of COMPAQ DOS. Four DOS directories are required.

The network supervisor plans to install word processing, electronic mail, a spreadsheet, and a database application. A parent APPS directory is planned, along with a subdirectory for each application's program files. The electronic mail program creates its own directory structure.

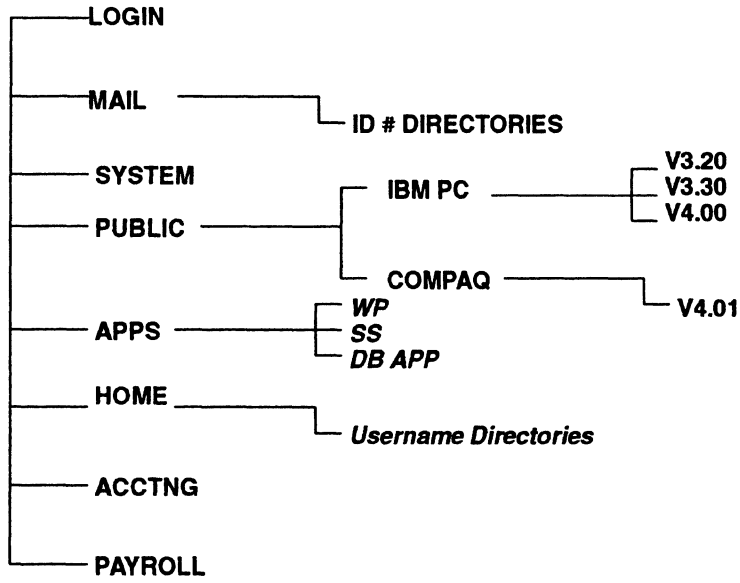
The HOME directory provides personal work space for users in username subdirectories.

The ACCTNG directory contains data files for all applications used by the accountants.

The PAYROLL directory contains the data record files for the payroll database.

The network supervisor should first diagram the directory structure (as shown below) and then record the directories on the Directories Worksheet.

Directory structure example



Planning the users and groups

Use the Users Worksheet and copies of the Group Worksheet as you complete this section.

Planning the users and groups involves the following tasks:

- Determining usernames
- Planning hybrid users (optional)
- Planning workgroups (optional)
- Planning groups
- Deciding which utility to use for user definition
- Deciding whether to install Accounting
- Planning defaults for defining users

The network supervisor allows people to work on the network by defining them on the file server as users. A user has a username and a user account.

To simplify network administration, the network supervisor can define groups of users who use the same applications or perform similar tasks, or who have similar needs for information or printing.

When the file server is first brought up, the bindery already contains the users SUPERVISOR and GUEST and the group EVERYONE.

As network supervisor, you must define all other users and groups, unless you delegate those responsibilities to a workgroup manager.

Choose how much responsibility you want to delegate. You can organize workgroups or you can delegate account management to a user account manager without creating a workgroup.

For more information, see **Users**, **Groups**, **Workgroup manager,** and **User account manager** in *Concepts*.

Determining usernames

Make a list of everyone who will be working on the network. Decide the username form you will use, such as

- Given names (for example, GEORGE, JANENE, and HOWARD).
- Initials and surnames (for example, GELLIS, JMGRADY, and HCRASK).
- Surnames (for example, ELLIS, GRADY, and RASK).

If you assign initials and surnames, you are less likely to have problems with duplicate usernames.

Usernames can use any valid DOS character and can be up to 47 characters long. However, keep in mind that username directories are still limited to the 8 characters that DOS will display.

Planning hybrid users (optional)

Decide which users will be hybrid users.

A hybrid user is a user that can access both the DG/UX directory structure and the NetWare directory structure. The user account must already exist on both the AViiON host and NetWare sides, although the usernames and passwords do not need to match. You use the HYBRID utility to create a hybrid user after a DG/UX user account and a NetWare user account have been created.

The average Netware user doesn't need a hybrid account; a hybrid account is useful only to a DG/UX user on the AViiON host who needs access to the NetWare directory structure.

(See **Hybrid user** in *Concepts* for more information.)

Planning workgroups (optional)

Form workgroups (perhaps by organizational divisions) and delegate the tasks of managing accounts or creating users and groups. Each workgroup can be assigned a separate volume or directory.

Workgroups can be managed by either of the following:

- A workgroup manager, who can create new users and manage their user accounts
- A user account manager, who can only manage assigned users' accounts

SUPERVISOR has all rights over the file server. A workgroup manager shares those rights but is restricted to a specific area on the file server (a volume or directory, for example). A user account manager has rights over only those user accounts assigned by the network supervisor.

The system is flexible, and you can delegate as much responsibility as seems appropriate. For example, you do not need to create a workgroup to delegate account management. You can simply assign one or more users to a user account manager to manage.

Only existing users and groups can be designated managers. If you want managers to make trustee assignments, assign them the Supervisory right [S] in a volume or a directory reserved for the workgroup or in other directories the managed users need access to.

IMPORTANT: If you want the users created by your workgroup managers to belong to the group EVERYONE, you will have to let the

workgroup managers manage the group EVERYONE. When you designate a user a workgroup manager, that user manages the group EVERYONE by default.

If you designate a workgroup manager for a workgroup, you must designate that user (or group) as workgroup manager of a user (or group), and then assign the workgroup manager the **S**upervisory right [S] to a volume or a directory reserved for the workgroup.

The workgroup manager can then set the system defaults and create the users and groups for the workgroup. The workgroup manager can also manage the user accounts and create new workgroup members when needed.

Or, if you want to set up the network without assistance, create all the users and groups and then assign them to designated workgroup managers. The effect is the same as if the users and groups had been created by workgroup managers, since the workgroup managers can manage their accounts. The workgroup managers can create additional users and groups as needed.

On the other hand, if you prefer not to delegate the right to create new users, create all users and groups and then assign the users and groups to User Account Managers (with or without workgroups). To allow the User Account Manager to make trustee assignments, assign the **S**upervisory [S] right in the volume or directory reserved for the workgroup.

For information, see **Workgroup manager** and **User account manager** in *Concepts*.

Planning groups

Regular network groups are organized within the pool of users (or within workgroups) to simplify system administration.

Groups are created on the file server as empty sets, and then members are added. A user can belong to a maximum of 32 groups. Decide which groups to create. Consider the following criteria:

Applications used — You can plan a group for each application (for example, WPUSERS for a word processing application).

Job responsibilities — You can plan groups for shared job responsibilities (for example, PAYCLERK for payroll data entry clerks).

Deciding which utility to use for user definition

Three utilities allow you to define users: SYSCON, MAKEUSER, and USERDEF. You can create users one at a time in SYSCON after the system defaults are set. You can create multiple users by creating and executing a MAKEUSER file (similar to a batch file) or by creating a USERDEF template that defines the parameters for multiple usernames you enter for processing.

For a discussion of the advantages and disadvantages of each utility, see "Utilities for Creating Users and Groups" under **Users** in the *Concepts* manual.

The setup procedure in this manual is based on creating users in the SYSCON utility. See "Set up the users with SYSCON" for specific instructions. The User Defaults Worksheet is designed to be used with SYSCON, it but can also be used with MAKEUSER and USERDEF.

If you prefer to use either the MAKEUSER or USERDEF utility, see *Utilities* for information to help you plan a MAKEUSER file or a USERDEF template.

After the NetWare user account is created, you can use the HYBRID utility to make the user a hybrid user.

Users and groups example

The network supervisor for the file server acme started with a list of users and their job titles, including the following:

Susan R. Leiter, vice president

Sue Ann Graves, payroll manager
George Ellis, supervisor, payroll clerks
Dan P. May, payroll clerk
Judith L. Burns, payroll clerk

Hal C. Rask, accounting supervisor
Jane M. Grady, accountant
Sam H. Black, accountant
Gamal H. Beltagi, accountant
John A. Parker, accountant

The network supervisor plans to use initials and surnames for usernames, such as the following:

SRLEITER
SAGRAVES
GELLIS
DPMAY
JLBURNS
HCRASK
JMGRADY
SHBLACK
GHBELTAGI
JAPARKER

The network supervisor plans to create the following groups based on applications used, job responsibilities, and information needs:

SPREADSHEET for accountants using a spreadsheet application

WPUSERS for the vice president, manager, supervisors, and accountants

PAYROLL for the manager and payroll supervisor

PAYREAD for the vice president and GUEST (who will be assigned a password)

PAYCLERK for payroll clerks who enter data

The network supervisor plans to assign the payroll manager as the User Account Manager for all payroll clerks after they have been created as users.

The entry on the Users Worksheet for Dan P. May records the following decisions (directories required for application–based groups are not listed):

Username:	DPMAY
Application Used:	Database
Groups:	PAYCLERK
Access to Directories:	SYS:HOME\DPMAY SYS:PAYROLL
Time Restrictions:	M–F 7am–6pm SAT 7am–1pm
Station Restrictions:	[00001b02757A] [32]
Managed by:	SAGRAVES
Operator or Manager:	n/a

The Group Worksheet for the WPUSERS group records the following decisions:

Group Name:	WPUSERS
Basis of Group:	word processing
Full Name:	word processing users
Managed by:	SAGRAVES
Access to Directories:	SYS:APPS\WP SYS:APPS\WP\SETUP
Trustee Directory Assignments:	SYS:APPS\WP [RF] SYS:APPS\WP\SETUP [RWCEMF]
Access to Files:	n/a
Trustee File Assignments:	n/a

Usernames of Members:

SRLEITER
SAGRAVES
GELLIS
HCRASK
JMGRADY
SHBLACK
GHBELTAGI
JAPARKER

Deciding whether to install Accounting

Use the User Defaults Worksheet as you complete this section. Record your decisions about the Accounting feature.

You can select the Accounting feature as an option in SYSCON. We suggest that for your initial setup you make only the following decisions:

- Whether to install the Accounting feature
- What initial account balance you want for all users if you do install Accounting

By installing the Accounting feature, you can use auditing utilities to keep track of how often users log in and log out. This function is automatic when you install Accounting on your file server. You can track users without assigning account balances.

You can also use Accounting to compute charges for file server services. To determine your charge rate, monitor your file server for two or three weeks. Then set a charge rate based on your costs and the amount you must recover over a fixed period. See "Account balance" for suggestions on account balances for users. For more information, see "Accounting" under **SYSCON** in *Utilities and* **Accounting** in *Concepts*.

On the User Defaults Worksheet, record whether you want to install the Accounting feature. If you do, you can also assign an initial account balance for system defaults.

Accounting example

The network supervisor for the file server acme plans to install the Accounting feature to monitor how often users log in and log out. No account balance or limits will be assigned to users. However, after a period of monitoring the file server, the supervisor will also use Accounting to apportion network costs between the accounting and payroll departments.

Planning defaults for defining users

Use the Users Worksheet, the User Defaults Worksheet, and copies of the Group Worksheet as you complete this section.

You can set the following system defaults in "Supervisor Options" of SYSCON before you create users and user accounts:

- Default Account Balance/Restrictions
- Default Time Restrictions
- Intruder Detection/Lockout

All users created after the defaults are set receive the same default user characteristics. You can change the account balances and restrictions by resetting the defaults when you create additional users, or you can modify individual user accounts after the users have been created.

Even if you define users by creating a MAKEUSER file or a USERDEF template, you can still incorporate the planning decisions you make in SYSCON. Some features, such as station restrictions, must be assigned individually after users are created.

Follow these steps to plan defaults for defining users.

1. Determine default account balance/restrictions

   "Default Account Balance/Restrictions" in SYSCON displays the following initial settings:

```
        Default Account Balance/Restrictions

Account Has Expiration Date:        No
  Date Account Expires:
Limit Concurrent Connections:       No
  Maximum Connections:
Create Home Directory for User:     No
Require Password:                   No
  Minimum Password Length:
Force Periodic Password Changes:
  Days Between Forced Changes:
  Limit Grace Logins:
    Grace Logins Allowed:
Require Unique Passwords:
Account Balance:                    0
Allow Unlimited Credit:             No
  Low Balance Limit:                0
```

The defaults set no restrictions. If you want security to be tighter, you must change the default settings. Each field in this window is described below.

Account Has Expiration Date

If you plan to set up temporary accounts, set this field to Yes. "Date Account Expires" is set by accepting the default (the first day of the next month) or by typing in a new date. The account will be automatically disabled on the expiration date at 12:01 a.m.

Limit Concurrent Connections

If you want users to log out of one workstation before logging in to another, set this field to Yes. If you choose to limit the number of workstations a user can be logged in to, set the "Maximum Connections" by typing in the desired number of workstations.

Home Directories for Users

If you want NetWare to create a home directory for users as you create them, change the option to Yes.

Passwords

We recommend that you require passwords, and we suggest that you accept the following defaults that appear when you set this field to Yes.

- Minimum Password Length: 5 characters
- Force Periodic Password Changes: Yes
- Days Between Forced Changes: 40
- Limit Grace Logins (the number of times a user can log in with an expired password): Yes
- Grace Logins Allowed: 6

Require Unique Passwords (prevents users from recycling favorite passwords): Yes

If you do not want to accept the default on any parameter, you can enter a new value.

Account Balance

This field appears only if you install Accounting. Leave the balance at the default if you do not plan to monitor or charge for the use of file server resources. If no charge rates have been set, the account balance is irrelevant. However, when a charge rate is set, the account balance is reduced when the specified network resource is used.

If you plan to charge for the use of network resources, assign an initial account balance. We suggest you start with 1,000 units of credit.

Determine how much you will charge per month based on connect time, blocks read, or blocks written.

When the user works on the network, the balance is reduced according to the charge rate you set for the specified resource.

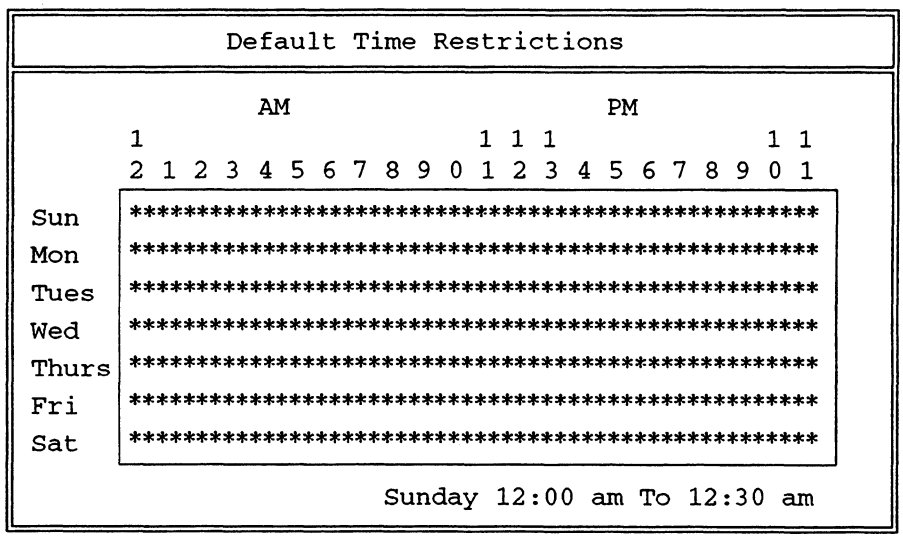
You can set credit limits before you establish charge rates. The limits do not restrict user accounts until the charge rates are in effect.

The default setting for "Allow Unlimited Credit" is No. If charge rates have been established, users cannot continue to "charge" on their accounts once the balance is depleted. If you want to allow unlimited credit, you must change the setting to Yes.

If you do plan to charge for file server services, you can limit how low the account balance can go by entering a new number (even a negative number) for the "Low Balance Limit" field.

2. Determine default time restrictions

   For increased security, specify the hours that users can log in to the file server. Time restrictions are set by days of the week in half–hour blocks.



If you want all users to have the same restrictions, assign "Default Time Restrictions" in SYSCON.

If you want only particular users restricted, set time restrictions when you set up each user's account.

3. Determine intruder detection/lockout capabilities

   For maximum security, we recommend that you activate "Intruder Detection/Lockout." After an intruder makes several unsuccessful attempts to log in using an incorrect password, the file server locks the intruder out.

```
                Intruder Detection/Lockout

Detect Intruders: No

Intruder Detection Threshold
Incorrect Login Attempts:
Bad Login Count Retention Time:  Days   Hours   Minutes

Lock Account After Detection:
   Length Of Account Lockout:    Days   Hours   Minutes
```

The intruder detection/lockout fields are described below.

Intruders

If you want to activate "Intruder Detection/Lockout," set this field to Yes.

Intruder Detection Threshold

You must set the threshold by specifying the number of "Incorrect Login Attempts" the file server accepts before disabling the account. The default is 7 to allow for normal typing errors.

"Bad Login Count Retention Time" is the amount of time the file server monitors incorrect login attempts after the last allowed incorrect login attempt was detected. The default is set for 30 minutes.

Lock Accounts After Detection

When "Intruder Detection/Lockout" is activated and the threshold for incorrect login attempts is exceeded, the account is locked automatically. The default for "Length of Account Lockout" is 15 minutes, but you can specify a longer period of time to keep an account locked.

SUPERVISOR can "unlock" disabled accounts at any time. However, the network supervisor needs a back door into the system in case an intruder locks the SUPERVISOR account. See **SUPERVISOR** in *Concepts* for suggestions.

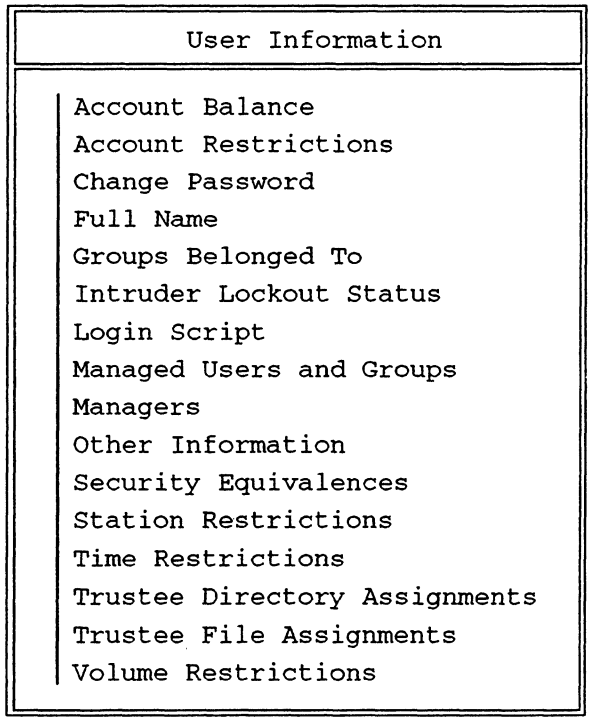
When you have decided what settings you want to make in the "Default Account Balance/Restrictions," "Default Time Restrictions," and "Intruder Detection/Lockout" fields, record your planning decisions on the User Defaults Worksheet. To create users in separate groups or workgroups with different default settings, use a separate copy of the worksheet for each group or workgroup.

4. Plan individual account features

   Use the Users Worksheet and your Group Worksheets as you complete this section.

   You must set the options and restrictions for which no system default applies. Account restrictions that can be assigned with system defaults can also be assigned individually. You may prefer to add or remove restrictions set with system defaults.

   When you select a user from the list of existing users, the following menu appears (all options are explained on the following pages):



Account Balance

This option appears if you have installed Accounting. If you did not assign a default initial account balance, you can assign account balances and credit limits to users individually.

Account Restrictions

This option allows you to set account restrictions individually if you do not set them as defaults.

If you define users initially with system defaults, you can modify particular user accounts by adding or removing restrictions after the users have been created.

The following form appears when you select "Account Restrictions:"

```
   Account Restrictions For User SQLEITER

Account Disabled:                        No
Account Has Expiration Date:             No
   Date Account Expires:
Limit Concurrent Connections:            No
   Maximum Connections:
Allow User To Change Password:           Yes
Require Password:                        No
   Minimum Password Length:
Force Periodic Password Changes:
   Days Between Forced Changes:
   Date Password Expires:
   Limit Grace Logins:
      Grace Logins Allowed:
      Remaining Grace Logins:
Require Unique Passwords:
```

To restrict an individual user, modify the default settings shown above. (You can disable an account by changing the "Account Disabled" field to Yes.)

Change Password

You can assign a password to a user. If you are upgrading or creating multiple users, you can assign the same password to all users in a workgroup and they are prompted to change their passwords when they log in for the first time. (Your system is secure only until users know the initial password or the password pattern.) If you assign passwords and require periodic changes to the passwords, the users are prompted to changed their passwords the first time they log in.

Full Name

You can record the user's full name as it appears on the Users Worksheet.

Groups Belonged To

You can assign the user to appropriate groups. Later, when you add a new user to the file server, we suggest you use this field to assign membership in appropriate groups. However, the initial setup is more convenient if you access the group name and then assign users as members. Instructions for doing so are included in "Set up the users with SYSCON."

Intruder Lockout Status

This option appears only if you activate the Intruder Detection/Lockout feature. No input is necessary. Later, you can select this option to view a record of any unauthorized attempts to log in using a particular user account.

Login Script

After you create users, select this option to access an entry box for each user's login script. You can either create a login script or copy and modify an existing user's login script.

Managed Users and Groups

With this option, you can assign users and their accounts to a user account manager. Indicate this in the "Operator or Manager" column of the Users Worksheet.

Managers

With this option, you can designate a user account manager. Record the user account manager's username in the "Managed by" column of the Users Worksheet.

Other Information

No input is necessary. Later, you can use this option to view the user's ID number, the date and time of the user's last login, and whether the user has been designated as a file server console operator.

Security Equivalences

With this option, you can assign a user any appropriate security equivalences (optional). Use caution. A security equivalence gives a user access to all directories and files of another user, so this option is best used to assign rights only temporarily.

Station Restrictions

To limit the physical locations that a user can log in from, set restrictions for each user; otherwise, there are no restrictions.

To restrict a user to a particular workstation, you need the network and node (station) addresses for each workstation. For a list of these addresses, refer to the Workstation Configuration Worksheet. Record the addresses in the "Station Restrictions" column of the Users Worksheet.

Time Restrictions

Time restrictions can be set for each user in the same way that "Default Time Restrictions" are set. If you prefer not to restrict all users, record the allowable times for particular users in the "Time Restrictions" column of the Users Worksheet.

Trustee Directory Assignments

You can assign a user as a trustee of a directory. If you specify a directory that does not exist, SYSCON creates the directory. (When possible, make trustee assignments to groups rather than to individual users.)

Trustee File Assignments

To control access to files, you can make a user a trustee of particular files. (When possible, make trustee assignments in directories rather than in files.)

Volume Restrictions

This feature is not supported in this version of NetWare.

When you have decided what settings you want for individual users or what modifications you want to make to user accounts, record your planning decisions in the appropriate spaces on the Users Worksheet.

User definition defaults example

The network supervisor for the file server acme recorded the following decisions on the User Defaults Worksheet and the Users Worksheet:

- User accounts have no expiration date.
- The initial account balance will be set to 1000 units. Unlimited credit will be allowed while network use is monitored.
- Concurrent connections will be limited to two workstations.
- Intruder Detection/Lockout will be activated. The threshold default will be accepted. Bad login count retention time will be set to one hour. After intruders are detected, user accounts will be locked for 12 hours.
- Passwords will be required. Password defaults will be accepted.
- Time restrictions will be set individually for payroll clerks and be limited to the hours between 7 a.m. and 6 p.m., Monday through Friday.
- Station restrictions will be set to limit management users to two workstations. Other users will be limited to their own workstations.

Planning the network security

Use the Directories Worksheet, the Trustee Directory Security Worksheet, and the Trustee File Security Worksheet as you complete this section.

Planning the network security involves the following tasks:

- Planning rights security for users and groups
- Planning attribute security for directories and files

Although NetWare security is flexible and can be used in complex ways, we recommend a simple security setup and suggest appropriate security for different kinds of directories and files. You can implement more complex solutions as your network evolves.

Security for directories and files is controlled by rights and attributes.

Rights security applies to users individually and collectively and controls which directories, subdirectories, and files a user can access and what work the user is allowed to do with those directories, subdirectories, and files.

Attribute security applies to directories, subdirectories, and files and determines whether they can be viewed, modified, shared, renamed, or deleted. Attributes take precedence over rights.

Planning rights security for users and groups

Rights security is controlled by the Inherited Rights Mask and trustee assignments.

Inherited Rights Mask

An Inherited Rights Mask is assigned to each directory or file when it is created. For basic security setup, you do not need to modify the Inherited Rights Mask. For information on the effects of modifying the mask, see **Security** in *Concepts*.

Trustee assignments

When users or groups are granted rights to specific directories or files, the users or groups become trustees of those directories or files. The sum of the rights becomes the trustee assignment.

A trustee assignment allows a user or group member to use the directory or the file in a particular way (for example, only for reading). The network supervisor (or a user with the Access Control right) selects the appropriate rights to assign to users or groups in each directory or file.

Trustee rights

The same trustee rights control access to directories and files in both trustee assignments and Inherited Rights Masks. Each right is represented by an initial letter, and the letters are enclosed in brackets: [SRWCEMFA].

Trustee Rights	
S	Supervisory
R	Read
W	Write
C	Create
E	Erase
M	Modify
F	File Scan
A	Access Control

Hybrid users

NetWare runs as a process with *root* privileges on the AViiON server. Because of this, protections and restrictions imposed by the system supervisor on a hybrid user's DG/UX account can be bypassed by the hybrid user's NetWare account. The AViiON system supervisor cannot impose restrictions on the NetWare account. For the system to remain secure, the NetWare system supervisor must also place restrictions on the hybrid user's NetWare account.

System-created directories and files

The system makes the trustee assignments. The system automatically makes the following trustee assignments to the group EVERYONE in the following directories:

PUBLIC [RF]
MAIL [C]

DOS directories

For DOS directories (or any directory) in the SYS:PUBLIC directory, the system automatically assigns the Read and File Scan rights [RF] to the group EVERYONE in SYS:PUBLIC.

Application directories

If you create application directories in the SYS:PUBLIC directory the Read and File Scan rights [RF] apply in the application directories. (This is because the group EVERYONE already has these rights in SYS:PUBLIC).

If you create a parent directory for applications, assign the File Scan right [F] to the group EVERYONE for that directory.

In the application directories themselves, whether in the parent directory or in SYS volume, assign the Read and File Scan [RF] rights to either the group EVERYONE or to the groups you have formed for application use.

IMPORTANT: If you have an application that creates extra files (such as backup files), assign each user the Create [C] right in the directory where the application creates those files. If the application needs to delete and recreate files, assign each user the Erase right [E].

Home or username directories

Each user needs all rights to personal work space. Assign each user (except GUEST) the Supervisory right [S] in the appropriate username directory. If you plan to provide personal work space for temporary users in a GUEST directory, assign GUEST the Read, Write, Create, Erase, and Modify rights [RWCEM]. Since the GUEST directory provides personal work space, assign the Modify right [M]. (Use caution in assigning GUEST the Access Control [A], Supervisory [S], and Modify [M] rights.)

Database directories for data files

If you have planned groups based on job responsibilities, make trustee assignments of at least the Read, Write, Create, Erase, Modify, and File Scan rights [RWCEMF] to the groups that need to modify the data files in database applications. Some database programs will require all rights except Supervisory [S]. For groups that only need to view information, you can assign the Read and File Scan rights [RF].

Work directories

Assign the Read, Write, Create, Erase, and Modify rights [RWCEM] to the groups that need to modify data files. For groups that only need to view information, you can assign the Read and File Scan rights [RF].

Batch file directories

Assign the Read and File Scan rights [RF] to the group EVERYONE.

Examine each directory you have listed on the Directories Worksheet. Then follow the decision process below for each directory.

1. Decide which groups or users need access to the directory.
2. Decide whether the group or user needs to view the files in the directory.
3. Decide whether the group or user needs to modify the files in the directory.
4. Decide what else the group or user needs to do.
5. If you have files for which you want to make a separate trustee assignment, repeat the decision process for those files.

When you have determined the most appropriate NetWare security, record the settings you want for trustee assignments on the Trustee Directory Security Worksheet. If you want to assign trustee rights separately for particular files, record the trustee assignments you want to make on the Trustee File Security Worksheet.

For more information, see "Rights Security" and "Effective Rights" under **Security** in *Concepts*.

Planning attribute security for directories and files

Attribute security assigns properties to individual directories or files. Each attribute is represented by its initial letter(s), and the letters are, by convention, enclosed in brackets.

Directory and file attributes

Attrib–utes	Letter	Direc–tory	File	Description
Archive needed	A		✓	• Identifies files modified after last backup. • Assigned automatically
Copy Inhibit	C		✓	• Prevents MacIntosh users from copying a file • Overrides Read and File Scan rights • Modify right required to remove this attribute
Delete Inhibit	D	✓	✓	• Prevents users from erasing directories or files • Overrides Erase rights • Modify right required to remove this attribute
Execute Only	X		✓	• Prevents copying or backing up files • Attribute cannot be removed • Assign only to program files (with .EXE or .COM extension) • Keep a duplicate copy of these files in case they get corrupted NOTE: Some programs flagged Execute Only will not execute properly.
Hidden	H	✓	✓	• Hides directories and files from DOS DIR scans and prevents them from copying or deleting • Directories and files appear in NetWare NDIR scan if user has the File Scan right.

Attrib–utes	Letter	Directory	File	Description
Indexed	I		✓	• Allows quick access to big files • Automatically assigned to files with over 64 regular FAT entries. • Can be set, but setting has no effect.
Purge	P	✓	✓	• If a file is tagged or resides in a directory tagged with this attribute, purges the file as soon as it is detected *CAUTION: You cannot use SALVAGE to recover a purged file.*
Read Audit	Ra		✓	• Not currently used by NetWare. Can be set, but setting has no effect.
Read Only/ Read Write	Ro/Rw		✓	• Indicates whether a file can be modified. All files are automatically flagged Read Write when created, and can be modified unless the Read Only attribute is set. • Assigning Ro automatically activates Delete Inhibit and Rename Inhibit. • Modifying right required to remove Ro attribute.
Rename Inhibit	R	✓	✓	• Prevents users from renaming directories or files. • Modifying right required to remove this attribute.
Share-able	S		✓	• Allows several users to simultaneously access a file • Typically used in combination with Ro attribute

Attrib–utes	Letter	Directory	File	Description
System	Sy	✓	✓	• Assigned to system files and their directories, hides them from DOS DIR scans and protects them from copying or deleting. • If users have File Scan right, directories and files appear in NetWare NDIR scans.
Trans–actional	T		✓	• Activates the Transaction Tracking System (TTS). • Prevents data corruption by ensuring that either all or no changes are made to files being modified. • Especially helpful for database files
Write Audit	Wa		✓	• Not currently used by NetWare. Can be set, but setting has no effect.

Note that this version of NetWare does not support Transaction Tracking. The [T] attribute may be assigned, but will not affect anything.

Consider the following recommendations.

System–created directories and files

These files are automatically flagged Read Only [Ro], Delete Inhibit [D], and Rename Inhibit [R] by the system. No additional attributes are necessary.

DOS directories

Flag DOS files Read Only/Shareable [RoS]. The system automatically adds the Delete Inhibit [D] and Rename Inhibit [R] flags.

IMPORTANT: The [RoS] attribute should not be confused with [ROS] rights in earlier versions of NetWare.

Application directories

Flag application program files Read Only/Shareable [RoS]. To prevent anyone from copying software illegally, flag the principal executable file of each application Shareable/Execute Only [SX].

CAUTION: Not even SUPERVISOR can copy files flagged Execute Only [X]. Files flagged with this attribute can only be deleted. Do not use this file attribute unless you have a backup copy of your application program files. Additionally, be sure that neither your license nor the installation program for your application restricts the number of times you can copy the files to the network.

Directories for database data files

Files you want to be able to modify should be flagged Read Write/Shareable [RwS].

Modify rights are required for any files flagged Shareable [S] or Delete Inhibit [D].

If you have highly sensitive information in your database that you do not want remaining on the hard disk after it has been deleted, flag the directory Purge [P] so that the files in that directory are purged upon deletion. Such files cannot be recovered.

Work directories

Files you want to be able to read but not modify should be flagged Read Only/Shareable [RoS].

Batch file directories

Flag the files Read Only/Shareable [RoS].

When you have determined the most appropriate NetWare security, record the settings you want for file attributes on the Directories Worksheet.

For more information, see "Attribute Security" under **Security** in *Concepts*.

Security example

The network supervisor for the file server acme planned the following directory trustee assignments:

Directory trustee assignments example

Usergroup	Directory	Rights
Everyone	SYS:APPS SYS:HOMEGUEST	[F] [RWC SMF]
Each user	SYS:HOMEusername	[S]
GUEST	SYS:HOMEGUEST	[RWC EMF]
SPREADSHEET	SYS:APPSPREAD SYS:ACCTING	[RF] [RWC EMF]
WPUSERS	SYS:APPWP SYS:APPWPSETUP	[RF] [RF]
PAYROLL	SYS:APPDB APP SYS:PAYROLL	[RF] [RWC EMF]
PAYREAD	SYS:APPDB APP SYS:PAYROLL	[RF] [RF]
PAYCLERK	SYS:APPDB APP SYS:PAYROLL	[RF] [RWC EMF]
MJONES	SYS:APPDB APP SYS:PAYROLL	[S] [S]

Planning the login scripts

Use the two Login Scripts Worksheets as you complete this section. The worksheets provide space for planning the system login script and user login scripts (which you can customize for each user).

Planning the login scripts involves the following tasks:

- Planning for login script conventions
- Planning a system login script

Login scripts are similar to the AUTOEXEC.BAT file and execute when users log in to the file server. Actually, two login scripts execute: first a system login script then a user login script. Both are created in SYSCON.

The network supervisor uses the system login script to set an environment for all users. The system login script contains commands that

- Map network drives.
- Control program execution.
- Initialize environmental variables. (A user login script specifies the user's individual drive mappings and environmental variables.)
- Because the system login script executes first, if you map the same drive letter or number in both login scripts, the mapping in the user login script overwrites the mapping in the system login script.
- For security reasons, each user should have a login script, however minimal. Since the group EVERYONE has the Create right [C] in SYS:MAIL and user login scripts are stored in a numbered ID subdirectory of SYS:MAIL, anyone (including GUEST) knowing a user's numbered ID subdirectory could create a login script in that ID subdirectory if one did not already exist.

- The system login script should be created first. If you access SYSCON's entry box for a user login script and put in even a blank space, the system reads it as a user login script and the default login script is no longer executed.
- When no user login script exists, a default login script executes. This is the same login script you see when you log in to the file server as SUPERVISOR for the first time. We recommend using the default login script only temporarily. Creating a user login script prevents the default script from executing for that user.
- On the other hand, most mistakes made in system login scripts generate a message listing the error. Then you can access SYSCON to correct the mistake. The critical command is the mapping to the NetWare utilities in SYS:PUBLIC.

Planning for login script conventions

Login scripts require the command formats specified in Appendix A, "Login Script Commands." A command format provides patterns for using keywords, options, variables, spacing, delimiters, or other characters and punctuation.

Login script commands are not case sensitive; however, any identifier variables enclosed in quotation marks must be upper case and must be preceded by a percent (%) sign.

Only one command can be entered on each line and command lines cannot exceed 150 characters. To increase readability, we recommend that you use only 78 characters per line – the width of your screen.

When you enter login script commands, end each line by pressing the Enter key. Words that are wrapped automatically onto the next line (because the end of the line was reached) are still considered part of the command on the previous line.

To make your login script easy to scan, you should

- Group similar commands.
- Include comments to record the purpose of each command or group of commands. Comments made with REMARK and its aliases (REM, *, and ;) do not display when the login script executes. For additional information and examples, see **Login scripts** in *Concepts*. For an explanation of individual login script commands, see Appendix A, "Login Script Commands."

Planning a system login script

The Login Scripts Worksheet is organized by headings. The headings (discussed below) are REMARK comments. Include the comments that apply to your script file. You can rewrite the comments or you can write your own. Then you can add the commands that correspond to the headings.

Preliminary commands

If you want to use any of the following commands, place them at the beginning of a login script (commands that can be set to ON or OFF can be used more than once in a script):

DOS BREAK ON|OFF
MAP DISPLAY ON|OFF

Greetings

Display brief messages on user screens with

WRITE "*message***"**

Display login messages

Use the following commands with the filename to display text files:

FDISPLAY *filename*
DISPLAY *filename*

When you display text files, type PAUSE on the next line so users can read the text at their own pace.

Attach to other file servers

If you want all users to attach to another file server, include ATTACH with the file server name:

ATTACH *server*

If you form groups on the basis of which file servers users need to attach to, you can use the conditional IF...THEN with ATTACH:

IF MEMBER OF *"groupname"* **THEN ATTACH** *server*

NetWare utilities mapping

The Login Scripts Worksheet contains the mapping we recommend:

MAP INS S1:=SYS:PUBLIC

DOS directory mapping and COMSPEC

The Login Scripts Worksheet contains the mapping we recommend, but you must supply the directory path according to the directory structure you create.

COMSPEC should specify the same search drive that is mapped to the DOS directory.

See **DOS directories** in *Concepts* for examples.

Application directory mappings

Map a search drive to each application directory to which all users or any defined group needs access. For an application used by all users, use the next search drive (following numerical order).

If you use the MAP INSERT command (as in the mapping to SYS:PUBLIC) and specify the number of the search drive, the system automatically assigns the next search drive available.

If you formed groups on the basis of application use, use the IF...THEN conditional to provide only that group with the mapping. If you use IF...THEN to provide a group with two or more mappings, you must also use BEGIN...END.

If you need to provide several groups of application users with conditional mappings, we suggest you include the command MAP INSERT S16 to map the next available search drive to each directory. Because MAP INSERT inserts a new search drive using the next available number in the ordered sequence of search drives, one mapping will not overwrite another.

Put the series of mappings in the order of frequent use. List the most frequently used application group first and the least frequently used application group last.

Miscellaneous search drive mappings

Using the MAP INSERT command (with or without the conditional IF...THEN), include a search drive mapping to any directory where batch files or third–party utilities are stored.

Supervisor mappings

To provide mappings to SYS:SYSTEM and any other supervisor directories, complete the IF...THEN conditional included on the worksheet. If you have more than one mapping, you must also use BEGIN...END with IF...THEN.

Home or username directory mapping

Include a generic mapping (using the identifier variable %LOGIN_NAME for the directory name) to the home or username directory.

We suggest that you map the first network drive to the home or username directories. The first network drive is usually F, but if you have workstations that require some other drive letter as the first network drive, you can use *1 as a generic first network drive.

If you prefer to map the first network drive to some other directory but want users in their personal work space at the end of the login script, use DRIVE. For an explanation of personal work space in home or username directories, see **Directory structure** in *Concepts*.

Data or work directory mapping

Include mappings to data or work directories. If you formed groups on the basis of job responsibilities or information needs, use the IF...THEN conditional to provide only that group with the mapping.

If you have workstations that use a drive letter other than F as the first network drive, we suggest that you use generic drives such as *2 and *3 (and so on, following numerical order) to represent drive letters (which follow alphabetical order). Or see your DOS manual for information on the use of LASTDRIVE.

Default printer mappings or printing batch files

If you have formed groups on the basis of print queues, you can use the IF...THEN conditional with #CAPTURE and a queue specification (for an explanation, see "Run miscellaneous programs"). Or you can call up batch files to provide printer or print queue routing.

Display directory path at prompt

To display the directory path at the prompt, we suggest you include [DOS] SET PROMPT as it appears on the worksheet. See your DOS manual for information on the use of SET.

Display all current drive settings

If you want drive mappings displayed for users, include the commands that appear on the Login Scripts Worksheet.

Run miscellaneous programs

To execute an external program (a filename with a .BAT, .COM, or .EXE extension), use the pound (#) sign preceding the name of the executable file. The pound sign allows both external execution and a return to continue the login script. #COMMAND /C *filename* also executes a DOS batch file. You can also run an executable file from an EXIT command. (However, if you use an EXIT command in a system login script, the user login script does not run.)

System login script example

The network supervisor for the file server acme planned the following system login script:

```
rem preliminary commands
MAP DISPLAY OFF
BREAK OFF
FIRE 3
rem greeting
WRITE ""
WRITE "Good %GREETING_TIME, %LOGIN_NAME."
WRITE ""
WRITE "You have logged in to acme from Station
%STATION."
WRITE ""
rem display login messages
IF MEMBER OF "PAYCLERK" THEN
WRITE "Staff meeting Tuesday 10 a.m. in Conference
Room C"
FDISPLAY SYS:message\daily.msg
PAUSE
rem attach to other file servers
IF MEMBER OF "PAYROLL" THEN
ATTACH HISTORY/%LOGIN_NAME
rem NetWare utilities mapping
MAP INS S1:=SYS:PUBLIC
rem DOS directory mapping and COMSPEC
MAP INS S2:=SYS:PUBLIC/%MACHINE/%OS/%OS_VERSION
```

If you plan a menu to give users quick and convenient access to applications and programs, you can call up the menu from the user login script. For more information on creating menus, see **MENU** in *Utilities Reference*.

IMPORTANT: Using EXIT from the system login script will not allow the user login scripts to run.

Application environmental variables

Consult the documentation that accompanies the applications you plan to install on the network. Determine what user variables can be set with the DOS SET command and then plan the command syntax as it should appear in the login script. (See your DOS manual for information on using SET.)

Individual search drive mappings

If only one user will use a directory containing executable files, plan a search drive mapping for that user to the directory.

Individual drive mappings

If a directory is frequently used by only one user, plan a drive mapping for that user to the directory.

Execute a menu

You can call up a menu from the login script by exiting to a menu with EXIT as the last command in the login script or by using #MENU. (For instructions on creating menus, see **MENU** in *Utilities*.) If you use the EXIT command, the string that follows can be 14 characters or fewer. For more details see "EXIT" in Appendix A, "Login Scripts."

The menu script file (for example PAYCLERK.MNU or ACCOUNT.MNU) must be stored in a directory to which a search drive has been mapped. You can include commands similar to the following four examples:

```
EXIT "MENU account"
IF MEMBER OF "PAYCLERK" THEN
```

```
EXIT "MENU payclerk"
#MENU account
IF MEMBER of "PAYCLERK" THEN
#MENU payclerk
```

Or you can also exit to a batch file:

```
EXIT "COMMAND /C GO"
```

In the GO.BAT file, include

```
MENU payclerk
LOGOUT
```

The GO.BAT file should also be stored in a directory to which a search drive has been mapped.

User login script example

The network supervisor for the file server acme planned user login scripts such as the following. The comments are preceded by a semicolon (;), an alias of REMARK. User SRLEITER uses word processing for which a backup interval and a username are set. The electronic mail program requires a username and a password. A print job is configured to provide the user with the ability to print correspondence on letterhead stationery.

```
;application environment variables
SET WP = "/b-10/u-sql/"
SET USR = "SRLEITER"
SET PWD = ""
;print job configuration
#CAPTURE J=LTTRHEAD
;individual search drive mappings
MAP INS *4:=SYS:HOME/SRLEITER/MACROS
```

From the examples, determine the elements to include in your system login script and your user login scripts. Record the

commands for your system login script on the Login Scripts Worksheet (see Appendix B). Record the commands for your user login scripts on the second page of the worksheet under "Basic User Login Script."

Creating the directory structure

To create the directories you have planned, use either the DOS CD (Change Directory) and MD (Make Directory) commands or the NetWare FILER utility. Use the instructions in this section to create all of your file server's directory structure except username directories. If you create users with the SYSCON utility, you can create username directories in SYSCON at the same time. (If you create users with USERDEF, DOS directories and username directories are created automatically.)

Creating the directory structure involves the following tasks:

- Installing DOS on the network
- Creating directories
- Loading application program files and setting field attributes
- Flagging the principal executable file Execute Only
- Copying any necessary files onto the workstation boot diskettes
- Copying data files into directories
- Using FLAF or FILER to asssign file attribute security (optional)

There are four ways to create these directories:

- DOS. For supervisors with DOS experience, the MD and CD commands are direct and efficient.
- FILER. FILER is menu driven so that you can select from lists or insert new directory names to create directory structure level by level. See **FILER** in the *Utilities*.

- SYSCON. When you create users with SYSCON, you can create username directories when you set up user accounts. If you specify a directory that does not exist, SYSCON creates the directory. (Instructions are included in "Set up the users with SYSCON.")
- USERDEF. If you create users with USERDEF, USERDEF creates your DOS directories and username directories.

Installing DOS on the network

You can create all the DOS directories and load all the DOS files from one workstation on the network. If you completed the planning worksheets, you should have recorded the required DOS directories on the Directories Worksheet. See **DOS directories** in *Concepts*.

IMPORTANT: As you create DOS directories and copy the DOS files onto the network, make sure you comply with all copyright laws. Each workstation must boot with its own licensed copy of DOS or other client operating system.

1. Booting a network workstation

   Turn on the workstation. (The file server should be up and running with volume SYS mounted.)

   If you have not prepared boot files, see the *NetWare ODI for DOS Workstations* manual.

2. Log in to the file server as SUPERVISOR. Type

   LOGIN *fileserver*/**SUPERVISOR** ↵

   Replace *fileserver* with your file server's name.

   Information from the default login script, similar to the following, appears:

```
Good morning, SUPERVISOR

Drive A maps to a local disk.
Drive B maps to a local disk.
Drive C maps to a local disk.
Drive D maps to a local disk.
Drive E maps to a local disk.
Drive F:= file server/SYS:SYSTEM
Drive G:= file server/SYS:LOGIN
Drive Y:= file server/SYS:PUBLIC
SEARCH1  := Z:. [file server/SYS:PUBLIC]

F:\SYSTEM>
```

When you first log in to the file server as SUPERVISOR, no password is required. For increased security, we suggest you assign yourself a password in SYSCON when you create users and set up user accounts. Then when you log in, you are prompted to enter your password. For more information on SUPERVISOR account security, see **SUPERVISOR** in *Concepts*.

3. You are in the SYS:LOGIN directory. If your prompt does not display the directory path, type

   PROMPT PG ↵

4. Change to the SYS:PUBLIC directory.

5. Create the DOS directories. Create a directory for each version of DOS you plan to run on each workstation type.

   We suggest you name your DOS directories according to the following convention:

   SYS:PUBLIC/*machine*/MSDOS/*version*

   For each directory, replace *machine* with the six–letter long machine name of the workstation (such as IBM_PC

or COMPAQ) and *version* with the DOS version number (such as v3.30 or v4.00).

6. Load DOS files into the appropriate DOS directories. Make sure the new DOS directory is your current directory. Copy the files from the DOS diskettes, using the NCOPY command.

   NCOPY A:*.* ↵

7. Flag DOS files Read Only/Shareable.

   You must flag all DOS files to prevent users from corrupting the command files. Use the FLAG command:

   FLAG *.* RO S ↵

8. Repeat Steps 6. and 7. for each DOS directory you create on the file server.

Creating directories

Use the DOS MD command to create your directories. If you wish, you can use FILER. See **FILER** in *Utilities*.

Loading application program files and setting file attributes

To use third–party applications (such as word processing programs, spreadsheet programs, and database programs), load the program files into the directories you created for them.

Refer to the documentation for each application.

After the files are loaded into the appropriate directories, you must also set file attribute security.

For applications with network versions — If the third–party documentation includes instructions for loading the application on a network, follow those instructions. Then skip to the "Flagging the principal executable file Execute Only" section.

For non–network applications — If the documentation does not contain instructions for loading the application on a network, try the instructions for loading the application on a local hard disk. (Some hard disk load commands don't work on network drives. If this is the case, consult the dealer who sold you the application.)

Some applications have an install program that requires the program to be installed in a root directory (represented by the volume name in NetWare). NetWare allows you to map a "fake" root. For more information, see **MAP** in *Utilities*.

1. If you use the local hard disk instructions, check to see whether the program requires the hard disk drive letter to be C or D. Then map the drive letter that normally corresponds to a local hard disk to the directory you have created for the application.

   For example, suppose you created a directory for an application in SYS:PUBLIC. If the third–party

documentation instructs you to copy the files to C, type the following command at the DOS prompt:

MAP ROOT C:=SYS:PUBLIC*directory* ↵

The following message appears:

```
Drive C: currently maps to a local disk.
Do you want to assign it as a network drive?
(Y/N) Y
```

2. Press <**Enter**> to confirm.

3. Either continue to follow the instructions (in the third–party documentation) for installing files on a hard disk, or insert each third–party diskette into drive A and type

   COPY A:*.* C: ↵

4. Flag the application program files Read Only/Shareable.

   The default file attribute is Read Write. Use FLAG or FILER to change the file attributes of application files to Read Only/Shareable [RoS]. This will prevent users from deleting or corrupting the program files (.EXE or .COM files). When you flag a file Read Only, NetWare automatically assigns the Delete Inhibit and Rename Inhibit attributes. For more information, see "Attribute Security" under **Security** in *Concepts*.

   Type

   FLAG *.* RO S ↵

Flagging the principal executable file Execute Only

To prevent users from copying applications from the network, we suggest that you flag the principal executable file (for each application) Execute Only [X]. This can be done only in FILER.

IMPORTANT: Not even SUPERVISOR can copy files flagged Execute Only. Files flagged with this attribute can only be deleted.

Do not use this file attribute unless you have a backup copy of your application program files. Additionally, make sure that neither your license nor the installation program for your application restricts the number of times you can copy the files to the network.

1. Access FILER.

   When you access FILER, the current directory path is indicated in the screen header.

2. Choose "Select Current Directory" from the "Available Topics" menu.

   A "Current Directory Path" entry box similar to the following appears:

```
Current Directory Path
acme/SYS:LOGIN
```

3. Enter the directory path for the application directory that contains the program file.

If you know the directory path. Type the directory path in the entry box, or use the Backspace key to delete the current directory path and then type the directory path you want.

If you do not know the directory path. Press <**Insert**> and then select the directory path one level at a time. Begin with the list of "Network Directories" and continue the selection process until the appropriate directory path appears in the box. Then press <**Escape**>.

4. Press <**Enter**> to return to the "Available Topics" menu.

   The screen header reflects the new directory path.

5. Select "Directory Contents" to list the contents of the current directory.

   The list can contain both subdirectories and files.

6. Select the appropriate file from the "Directory Contents" list.

7. Select "View/Set File Information" from the "File Options" menu.

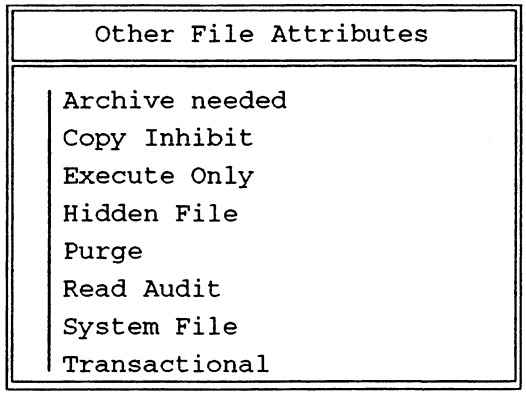
   A form similar to the following appears:

```
File Information for
REPORT.MAY

Attributes: [RoS-------------DR]

Owner: SUPERVISOR

Trustees:  (see list)

Current Effective Rights:
[SRWCEMFDA]

Size: 25600 bytes

Creation Date: October 31, 1990
Last Accessed Date: November 17,
1994
Last Archived Date: (NOT ARCHIVED)
Last Modified Date: November 17,
1994
```

8. The "Attributes" field is highlighted. Press **<Enter>** to view the "Current File Attributes."

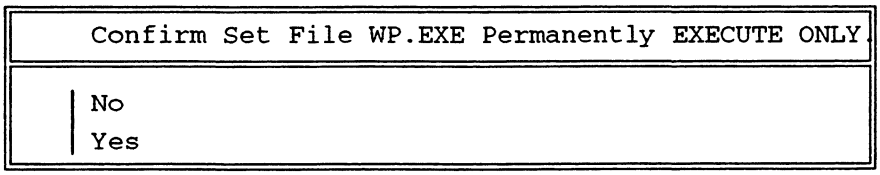
```
Current File Attributes

Delete Inhibit
Read Only
Rename Inhibit
Shareable
```

9. Press **<Insert>** to view "Other File Attributes."



10. Select "Execute Only" from the list of "Other File Attributes."

A confirmation box similar to the following appears:



11. Select Yes.

    "Execute Only" appears on the list of "Current File Attributes."

12. Exit FILER.

13. If you have additional applications to load, repeat the steps in both previous section, "Loading application program files and set file attributes," and in this, each time remapping drive C to the appropriate application directory.

Copying any necessary files onto the workstation boot diskettes

Check the third–party documentation to see if the application modifies or creates a CONFIG.SYS or an AUTOEXEC.BAT file. If this is the case, put those files on each user's boot diskette.

Copying data files into directories

Load data files into the directories you created for them.

To copy data files, insert each diskette into drive A and type

NCOPY A:*.* *path* ↵

Replace *path* with the directory path to the appropriate application directory (or if you mapped the directory to a drive, to the drive letter).

Using FLAG or FILER to assign file attribute security (optional)

For more information, see **FLAG** or **FILER** in *Utilities*.

Setting up the users with SYSCON

Setting up the users with SYSCON involves the following tasks:

- Installing the Accounting feature (optional)
- Setting system defaults for users
- Creating users
- Creating trustee rights
- Assigning trustee file rights
- Creating users and setting up user accounts
- Assigning password station and time restrictions to users
- Creating a username directory for each user
- Adding users to groups as members
- Designating a workgroup manager (optional)
- Designating user account managers (optional)
- Creating the system login script
- Creating user's login scripts

Installing the Accounting feature (optional)

Access SYSCON to install the accounting feature. Accounting is optional. However, Accounting must be installed if you want to assign an account balance to users when you set system defaults.

You can also use auditing utilities to monitor how often users log in and log out. Later you can choose which additional Accounting functions are suitable for your network.

If you need information to help you determine whether to install Accounting, see "Accounting" under **SYSCON** in *Utilities*; see also **Accounting** in *Concepts*.

1. Select "Accounting."

   The first time you select "Accounting" from the "Available Topics" menu, the "Install Accounting" confirmation box appears.

2. Select Yes.

Setting system defaults for users.

Use the User Defaults Worksheet as your guide in setting up system default restrictions in SYSCON.

If you did not complete the planning worksheets and need help determining what value to set for each parameter, refer to "Plan defaults for defining users;" see also **Users** in *Concepts*.

The system default restrictions are assigned to all users as they are created. However, default restrictions are set up initially so that no password or time restrictions apply. Unless you change the default restrictions, users have no password, login, account, or time restrictions.

Changes to the system defaults affect only user accounts that are created after the changes are made. Existing user accounts are not affected.

There are no default station restrictions. These must be established individually because users are restricted to specific workstations.

1. Select "Supervisor Options" from the "Available Topics" menu.

The "Supervisor Options" menu appears.

2. Select "Default Account Balance/Restrictions."

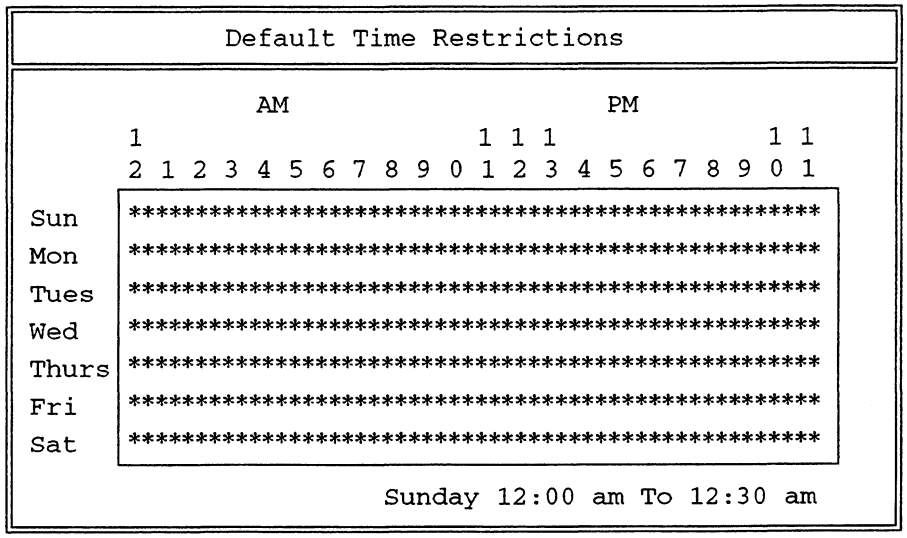
   If you have installed the Accounting feature, the "Account Balance" field appears:

```
        Default Account Balance/Restrictions

Account Has Expiration Date:        No
   Date Account Expires:
Limit Concurrent Connections:       No
   Maximum Connections:
Create Home Directory for User:     No
Require Password:                   No
   Minimum Password Length:
Force Periodic Password Changes:
   Days Between Forced Changes:
   Limit Grace Logins:
     Grace Logins Allowed:
Require Unique Passwords:
Account Balance:                    0
Allow Unlimited Credit:             No
   Low Balance Limit:               0
```

3. Enter the restrictions you have planned for your network.

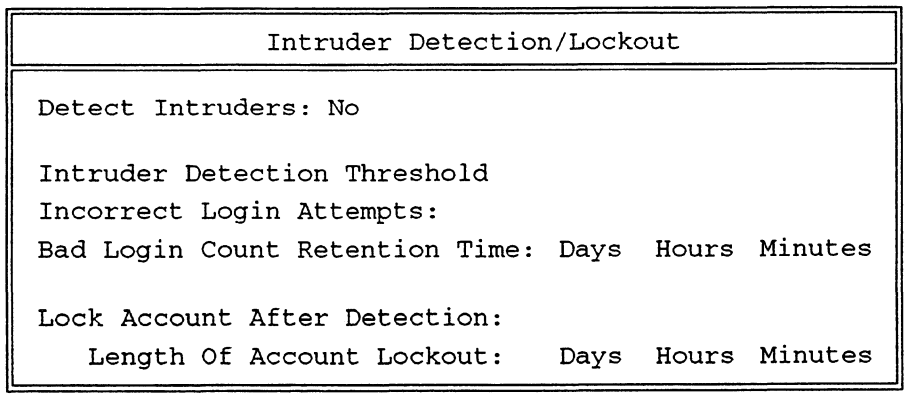
4. Select "Time Restrictions" in the "Supervisor Options" menu.

   Time is specified in half-hour blocks. To prevent users from logging in during a time block, delete the appropriate asterisks.



5. Select "Intruder Detection/Lockout" in the "Supervisor Options" menu and change the setting so the system detects intruders.

   You must also set the threshold for Intruder Detection and specify the length of time an account should be locked after an intruder is detected.



6. Exit SYSCON.

Creating groups

Use the Trustee Directory Security Worksheet, the Trustee File Security Worksheet, and copies of the Group Worksheet to create groups and assign group trustee rights to any directories or files. (Users can be added to a group only after both the users and the group have been created.)

If you completed the planning worksheets, you recorded the groups to create and which trustee assignments to make for each group.

If you did not complete the planning worksheets and need help determining what groups to create, see "Plan groups;" see also **Groups** and **Users** in *Concepts*.

If you plan to designate a workgroup manager to create the users and groups for the workgroup, you may want to create only those groups that apply across workgroup boundaries (for example, a group based on an application used by more than one workgroup).

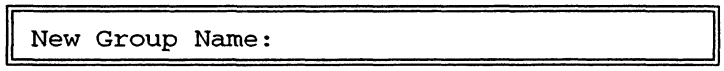
On the other hand, if you plan to designate a group as workgroup manager to create the users and groups for the workgroup, you should create the workgroup manager group when you create the system–wide groups.

In this case, assign the Supervisory right [S] in a volume or a directory reserved for the workgroup to the workgroup manager group.

1. Select "Group Information" from the "Available Topics" menu.

   A list of existing groups appears. (If no groups have been created, the group EVERYONE is the only group on the list.)

2. Press <**Insert**> and type the name of the new group in the entry box.

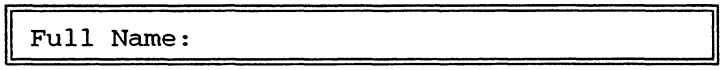


Then press <**Enter**>.

3. Select the group you just created.

4. Select "Full Name" from the "Group Information" menu.

5. Type the full name of the group in the entry box.



Then press <**Enter**>.

You are returned to the "Group Information" menu.

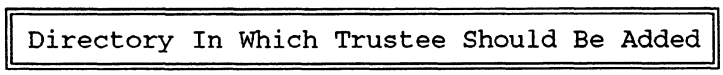
Assigning trustee rights.

1. To assign trustee rights for the group in a particular directory, select "Trustee Directory Assignments" from the "Group Information" menu.

The "Trustee Directory Assignments" list appears.

2. Press <**Insert**>.

An entry box appears.



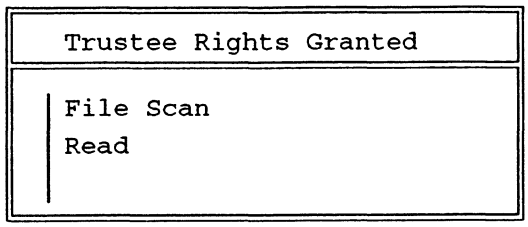
3. Enter the complete directory path.

If you know the complete directory path. Type the name of the directory in which you want the group to have trustee rights. (You must type the complete directory path.) Press <**Enter**>.

If you do not know the directory path. You can specify the directory path one level at a time. Press <**Insert**> and then select volume, directory, subdirectory, and so on. When the desired directory path appears in the box, press <**Escape**> then <**Enter**>.

The directory appears in the list of "Trustee Directory Assignments" with the default trustee rights, Read and File Scan [RF].

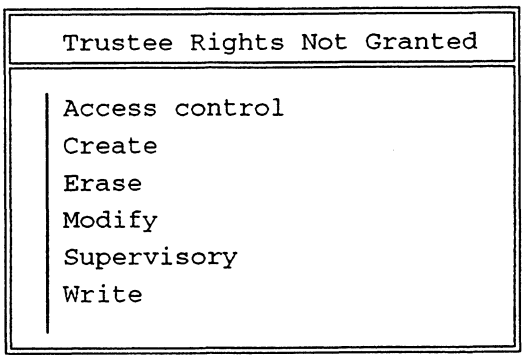
4. To add additional rights, press <**Enter**>.



The "Trustee Rights Granted" list appears.

5. Press <**Insert**> to view the list of trustee rights not granted.

6. Select the additional rights you want to grant from this list.



To add a trustee right. Select the trustee right you want.

To add more than one trustee right at once. Mark the rights you want to add using the Mark key (<**F5**> on most machines). Then press <**Enter**>.

The trustee directory right you granted now appears on the list of "Trustee Rights Granted." Press <**Escape**>.

7. Repeat the steps in both the previous section, "Creating Groups," and in this section to create groups and assign their trustee directory rights.

Assigning trustee file rights

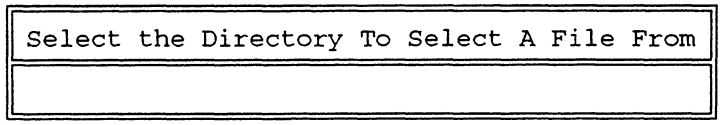
Use the Trustee File Security Worksheet to remind you what trustee file rights you planned to assign to each group.

1. To assign trustee rights for the group in a particular file, select "Trustee File Assignments" in the "Group Information" menu.

   The "Trustee File Assignments" list appears.

2. Press <**Insert**>.

An entry box appears.

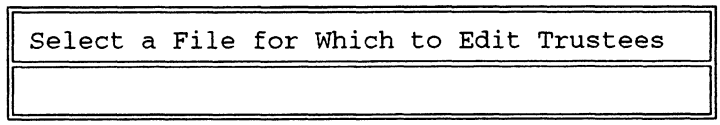


3. Enter the directory path.

   If you know the directory path. Type the name of the directory that contains the file in which you want the group to have trustee rights. (You must type the complete directory path.) Then press <**Enter**>.

   If you do not know the directory path. You can specify the directory p ath one level at a time. Press <**Insert**> and then select volume, directory, subdirectory, and so on. When the desired directory path appears in the box, press <**Escape**> and then <**Enter**>.

4. Select the filename.



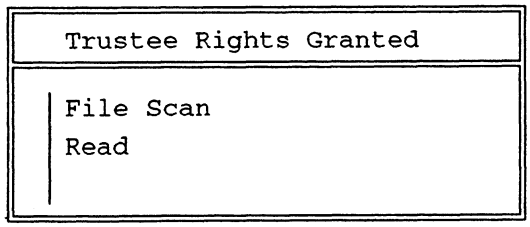
   If you know the filename. Type the filename you want the group to have trustee rights to. Then press <**Enter**>.

   If you do not know the filename. Press <**Insert**> and select the filename from the list that appears. Press <**Enter**> again.

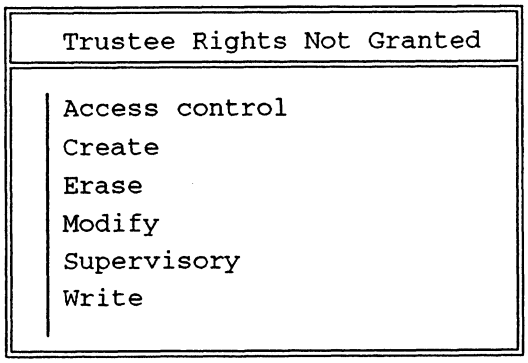
   The filename appears in the list of "Trustee File Assignments" with the default trustee rights, Read and File Scan [RF].

5. To grant additional rights, press <**Enter**>.

The "Trustee Rights Granted" list appears.



6. Press <**Insert**> to view the trustee rights not granted.
7. Select additional rights to grant from this list.



To add a trustee right. Select a trustee right.

To add more than one trustee right at once. Mark the rights you want to add using the Mark key (<**F5**> on most machines). Then press <**Enter**>.

The trustee file rights you grant appear on the "Trustee Rights Granted" list. Press <**Escape**>

8. Repeat Steps 1. through 7. for each file to which you want to assign trustee rights for a particular group.

Creating users and setting up user accounts

Use the Users Worksheet as a guide for creating users and setting up their accounts. You can also use the Trustee

Directory Security Worksheet and the Trustee File Security Worksheet to make trustee assignments to users. Refer to the Group Worksheets you completed to assign users to their respective groups.

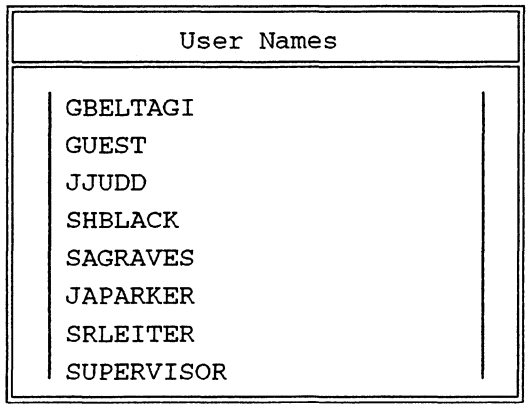
To delegate the responsibility of creating users and groups to workgroup managers, you must first create the workgroup managers.

To designate a user as a workgroup manager — Create the user and assign the Supervisory right [S] in a volume or a directory reserved for the workgroup. Then skip to the "Designating a workgroup manager (optional)" section. The workgroup manager can create users and groups for the workgroup.

To designate a group as a workgroup manager — Create the group and the users you plan to assign to the group. Assign the users as members of the group. Assign the group the Supervisory right [S] in a volume or a directory reserved for the workgroup. Then skip to the "Designating a workgroup manager (optional)" section. The members of the group can now create users and groups for the workgroup.

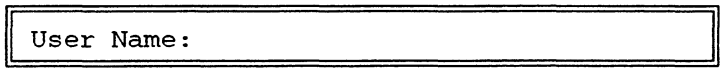
1. Select "User Information" from the "Available Topics" menu.

   A "User Names" list similar to the following contains the names of existing users. (If no users have been created, the list contains GUEST and SUPERVISOR.)



2. Press <**Insert**> to add a name to the list.

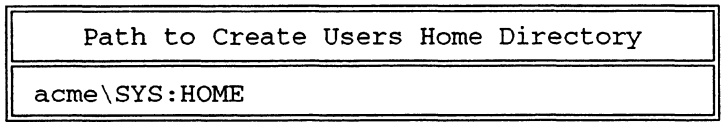
3. Type a username from the list of users you plan to create.



4. Press <**Enter**>.

   The username appears in the "User Name" list.

5. If you have set the system to create a home directory for each user, enter the directory path where all home directories will be stored (SYS:HOME, for example).



6. Repeat Steps 2. through 5. for each user.

Assigning password, station, and time restrictions to users

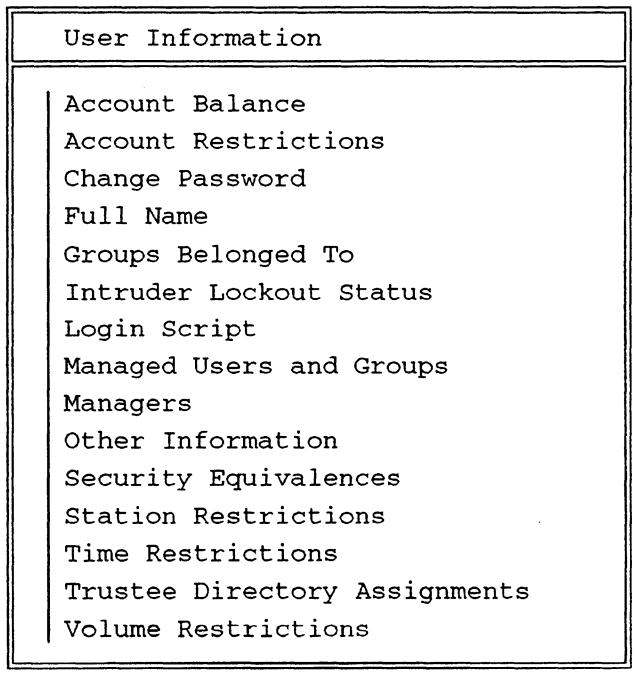
You must set those options and restrictions for which no system default applies.

If you did not set restrictions at the system level (such as time restrictions), you can set them to apply to particular users.

If you set system defaults, you can remove or assign them for particular users.

1. Select the new username in the "User Names" list.

   The "User Information" menu appears.



2. Highlight each appropriate option and type the correct information as necessary.

Refer to the User Defaults Worksheet to make the settings you planned.

A brief explanation of the options in the "User Information" menu follows.

Account Balance

This option appears only if Accounting is installed. If you did not assign an account balance with system defaults, assign the user an account balance to determine the amount of network services and resources the user is allowed to use.

Account Restrictions

If you did not assign password and login restrictions with system defaults, assign them for each user (optional). The form is similar to that for system defaults.

```
        Account Restrictions For User GAMAL

Account Disabled:                    No
Account Has Expiration Date:         No
  Date Account Expires:
Limit Concurrent Connections:        No
  Maximum Connections:
Allow User To Change Password:       Yes
Require Password:                    No
  Minimum Password Length:
Force Periodic Password Changes:
  Days Between Forced Changes:
  Date Password Expires:
  Limit Grace Logins:
    Grace Logins Allowed:
    Remaining Grace Logins:
Require Unique Passwords:
```

Change Password

Assign the user a password.

Full Name

Record the user's full name (optional). (The full name must be recorded if you want to use the FULL_NAME identifier variable for login scripts.)

Groups Belonged To

Although you can assign a user to a group through "User Information," the initial setup is more convenient if you access the group through "Group Information" after all users are created. The instructions are in the "Adding users to a groups as members" section.

Intruder Lockout Status

This option appears only if Intruder Detection and Lockout is activated, but it is not used when you first create a user. No input is necessary. Later you can use it to view a record of any unauthorized attempts to log in using this user account.

Login Script

Later you will either create a login script for the user or copy an existing user's login script and modify it. (Instructions for creating user login scripts are in the "Creating users' login scripts" section.)

Managed Users and Groups

Use this option to assign the user the right to manage specified user accounts and groups. (All members of managed groups must also be managed users.)

If you planned workgroups, select all the users and groups in the workgroup. The user you selected (or inserted) in the "User Names" list automatically becomes a user account manager when you use this option to assign users and groups.

If you do not want workgroup managers to create users and groups during the initial setup, use this option to assign the users and groups you create for the workgroup to the workgroup managers. The effect is the same as if the users and groups had been created by the workgroup manager. Workgroup managers have the right to create additional users and groups after the initial setup.

Instructions for assigning users and groups to a user account manager are also provided in the "Designating user account managers" section.

Managers

If you want to designate a user account manager to manage a user's account, you can assign one with this option. A user or a group becomes a manager simply by being assigned an account to manage.

Other Information

No input is necessary. You can use this option later to view the user's date and time of last login, disk space in use, user ID number, and whether the user has been designated as a console operator.

Security Equivalences

Assign the user any appropriate security equivalences (optional). Because a security equivalence gives one user access to all directories and files of another user, this is best used to assign a user temporary rights.

Station Restrictions

Specify the workstations a user can log in from (optional).

If you planned station restrictions, you should have recorded the network address and the node (station) address of each workstation on the Users Worksheet.

To display the addresses for all workstations logged in to the file server (after the network is in use), enter "USERLIST /A" at the command line.

Time Restrictions

If you have not set system defaults for time restrictions yet and you want to limit the times during which particular users can log in, use this option.

Instructions for restricting login times are under **SYSCON** in *Utilities*.

Trustee Directory Assignments

Assign a user as a trustee of the appropriate directories. Check the Users Worksheet and the Trustee Directory Security Worksheet to see which directories each user needs rights to.

Assigning trustee rights to groups is more efficient. You should assign trustee rights to users for only those directories they do not share with other users.

Trustee File Assignments

Assign a user as a trustee of the appropriate files (optional). To see which files a user needs rights to, check your Trustee File Security Worksheet.

Assigning trustee rights in directories is more efficient. When possible, make most trustee file assignments to groups; most trustee assignments should be to directories rather than to files.

Volume Restrictions

This feature is not supported in this version of NetWare.

3. When you have set the various options on the "User Information" menu, press **<Escape>** to return to the "User Names" list.

4. Repeat Steps 1. through 3. for each user.

Creating a username directory for each user

If you did not create username (home) directories either when you created other directories or as you created the users with SYSCON, you can follow these instructions to create a username directory for each user and assign all trustee rights in that directory.

IMPORTANT: You can also use these steps to give directory trustee assignments to users in directories other than their home directories.

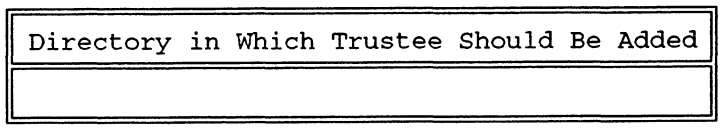
1. Select the user in the "User Names" list.

2. Select "Trustee Directory Assignments" from the "User Information" menu.

   The "Trustee Directory Assignments" window appears.

3. Press <**Insert**>.

   The following entry box appears:

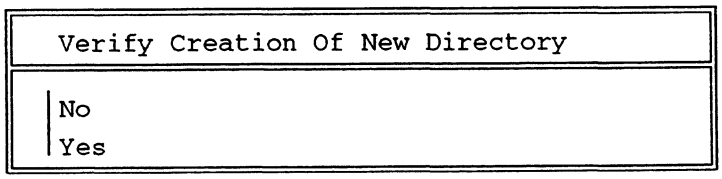


4. For the user you selected, type the complete directory path of the username directory (or directory to make the assignments in). Then press <**Enter**>.

   For example, to create the user's username directory in SYS:HOME, type

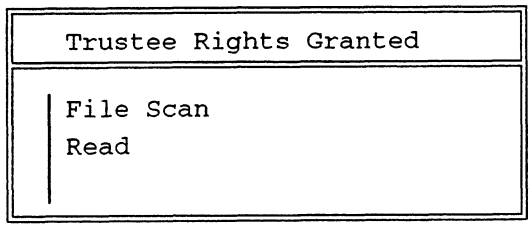
   SYS:HOME/*username* ↵

   The following confirmation box appears:



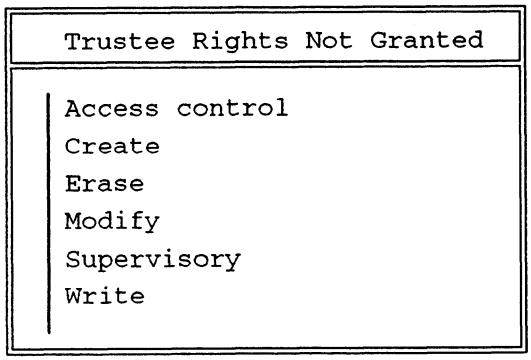
5. Select Yes.

6. Press <**Enter**> to display the "Trustee Rights Granted" in the directory.



The default trustee rights are Read and File Scan [RF].

7. Press <**Insert**> to display the list of trustee rights not granted.



8. Select "Supervisory" to assign the user all rights in the username directory.

   The Supervisory right is now displayed in the "Trustee Rights Granted" list.

9. Press <**Escape**> until you return to the "User Names" list.

10. Repeat Steps 1. through 9. to create a username directory for each user and assign the Supervisory right.

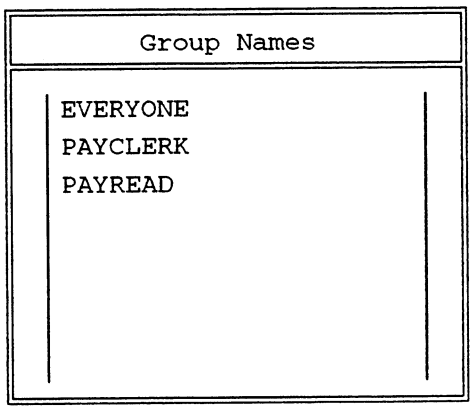
Adding users to groups as members

Use the Group Worksheet that you completed for each group to remind you which users belong to that group.

1. Press <**Escape**> until you return to the "Available Topics" menu.

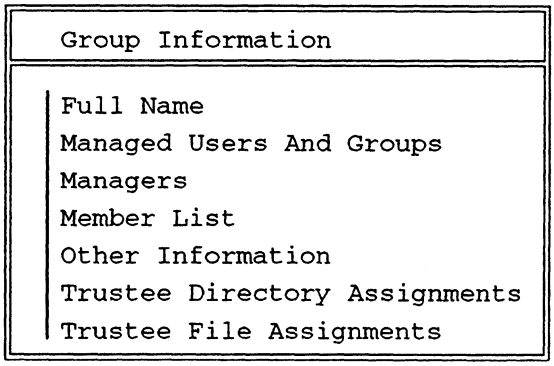
2. Select "Group Information."

   A "Group Names" list similar to the following contains the names of the groups you created:



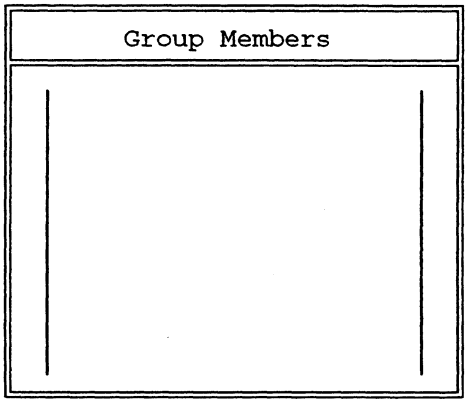
3. Select the group to which you want to add members.

   A "Group Information" menu appears for that group.

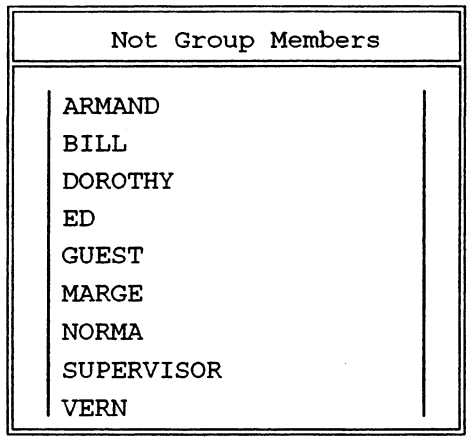


4. Select "Member List."

   The "Group Members" list appears.



5. Press **<Insert>** to view a list of users who are not members of the group.



6. From the list, select the users you want as members of the group.

   To add a member — Select the user you want.

   To add more than one member at once — Mark the users you want with the Mark key (<**F5**> on most machines). Then press <**Enter**>.

   The users you added to the group appear on the "Group Members" list. Users can belong to a maximum of 32 groups.

7. If you have more groups to fill, press <**Escape**> to return to the "Group Names" menu. Repeat Steps 3. through 6. for each group you created.

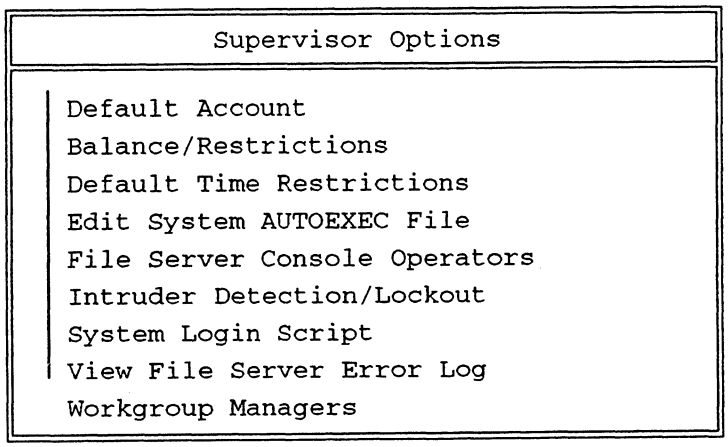
8. If you plan to designate workgroup managers or user account managers, press <**Escape**> to return to the "Available Topics" menu. Either continue to the next section, "Designating a work group manager (optional)," to designate a workgroup manager or skip to the "Designating user account managers (optional)" section to designate a user account manager.

Designating a workgroup manager (optional)

If you need planning information, see "Plan workgroups."

1. Select "Supervisor Options" from the "Available Topics" menu.

2. Select "Workgroup Managers" from the "Supervisor Options" menu.



A list of existing workgroup managers appears.

3. Press <**Insert**> to view a list of "Other Users And Groups."

Other Users And Groups	
ANATOL	(User)
ARMAND	(User)
BILL	(User)
DOROTHY	(User)
ED	(User)
EVERYONE	(Group)
GUEST	(User)

4. Select the user or the group you want to designate as workgroup manager.

   The user or the group you selected is now a workgroup manager and appears on the "workgroup managers" list.

5. Press <**Escape**> until you can select "User Information" from the "Available Topics" menu.

6. Select a workgroup manager.

7. Select "Managed Users and Groups" from the "User Information" menu.

   The workgroup manager will manage the group EVERYONE if the users to be managed are part of the group EVERYONE.

8. Press <**Insert**> and select the users or groups for the workgroup manager to manage.

Designating user account managers (optional)

If you need planning information, see "Plan workgroups."

1. Select a user account manager.

   For a user — Select "User Information" from the "Available Topics" menu. A list of existing users appears. Select the appropriate user from the list.

   For a group — Select "Group Information" from the "Available Topics" menu. A list of existing groups appears. Select the appropriate group from the list.

2. Assign users or groups to the user account manager.

3. Select "Managed Users and Groups" from either the "User Information" or "Group Information" menu.

   The list for "Managed Users and Groups" appears.

4. Press <**Insert**> to view a list of "Other Users and Groups."

5. Select the users or groups you want to assign to the user account manager.

   You can assign groups if all group members are assigned to the same user account manager.

Creating the system login script

Use the Login Scripts Worksheet as a guide for creating login scripts. The worksheet should contain a record of the commands you want in the system login script and in the user login scripts.

If you did not use the planning worksheets and need help determining what to put in your login scripts, see "Plan the login scripts;" see also **Login scripts** in *Concepts*.

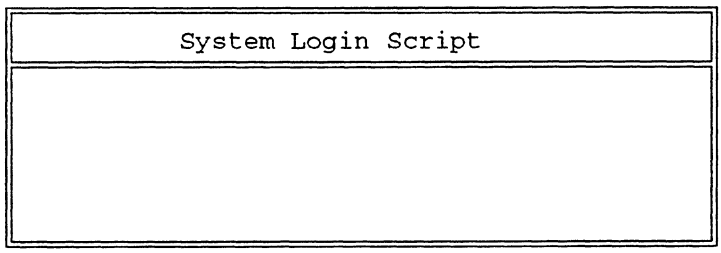
Login scripts are similar to the AUTOEXEC.BAT file and are executed as part of the login procedure. As network supervisor, you can create a system–wide login script that instructs all workstations to perform the same actions when users log in.

You can also create a login script for each user that executes after the system login script. A user login script specifies the drive mappings and environmental variables that apply only to that user. Users can modify their own login scripts in SYSCON if you allow them to change their own passwords. (The right to change a user's password includes the right to modify the user's login script.)

1. Select "Supervisor Options" in the "Available Topics" menu.

2. Select "System Login Scripts" in the "Supervisor Options" menu.

An empty "System Login Script" box appears:



3. In this box, type the login script commands you planned to include in your system login script.

4. When you finish entering the commands into the system login script, press <**Escape**> and then <**Enter**>.

Creating users' login scripts

Refer to the "Basic User Login Script" portion of the Login Scripts Worksheet for the commands you plan to include in each login script.

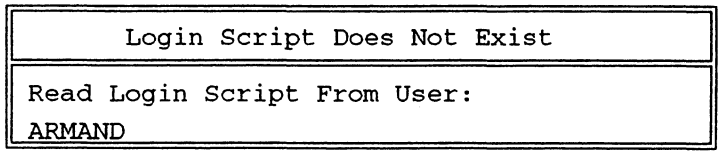
1. Select "User Information" from the "Available Topics" menu.

   The "User Names" list appears.

2. To access an individual login script, select the appropriate username.

3. Select "Login Script" from the "User Information" menu.

   If a login script has not been created for the user, a box (specifying the username you selected in Step 2.) similar to the following appears:



4. Press <**Enter**>. A user login script box appears.

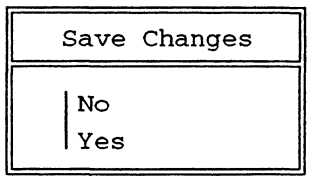
IMPORTANT: You can copy a login script from one user to another. See **SYSCON** in *Utilities* for instructions on copying all or portions of user login scripts from one user to another. After you have copied a login script, you can modify it as necessary.

5. Enter any drive mappings, environmental variables, and other login script commands you want for the user (excluding those already provided in the system login script).

IMPORTANT: Be sure not to include any commands in the login script that would log out the workstation from the primary file server.

6. When you have finished entering the commands, press <**Escape**>.

   The following confirmation box appears:



7. Select Yes and press <**Enter**> to save the login script changes. Then press <**Escape**> again to return to the "User Names" list.

8. Repeat Steps 1. through 7. to create a login script for each user.

Creating hybrid users

Creating hybrid users involves specifying the following:

- NetWare user account name
- Host user account name

IMPORTANT: All NetWare users on a Trusted DG/UX System must be hybrid users or they cannot log onto NetWare. You must make all NetWare users hybrid users *after* you install NetWare on a Trusted DG/UX System (as described in Appendix C) or change a regular DG/UX system with NetWare to a Trusted DG/UX System.

After NetWare user accounts are created, you can make some of these accounts into hybrid users. Note that an account for the user must also exist on the host system.

Use the HYBRID utility or SCONSOLE, and specify the NetWare user account name and the host user account name.

Where to go from here

To set up printing —See *Print Server*

To customize directory structure, user, or group information — See these commands in *Utilities*:

FILER
FLAG
FLAGDIR
GRANT
MAKEUSER
RIGHTS
SYSCON
USERDEF

End of Chapter

A Login Script Commands

Login scripts define the user environment. Each time a user logs in to a file server, the commands listed in the login script are executed in order. NetWare uses two kinds of login scripts: system–wide login scripts (referred to hereafter as system login scripts) and user login scripts.

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

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

For security reasons, each user should have a login script, however minimal. The group EVERYONE has the Create right [C] in SYS:MAIL, where users' login scripts are stored. If you do not create users' login scripts, anyone having access to the file server (including GUEST) could create a login script in a user's ID subdirectory.

If a user login script does not exist, a default login script is executed. This is the same login script you see when you log in to the file server as SUPERVISOR for the first time:

```
WRITE "Good %GREETING_TIME, %LOGIN_NAME."
MAP DISPLAY OFF
MAP ERRORS OFF
Rem: Set 1st drive to most appropriate directory.
MAP *1:=SYS:;*1:=SYS:%LOGIN_NAME
If "%1"="SUPERVISOR" THEN MAP *1:=SYS:SYSTEM
```

```
Rem: Set search drives (S2 machine-OS dependent).
MAP INS S1:=SYS:PUBLIC
MAP INS S2:=S1:%MACHINE/%OS/%OS_VERSION
Rem: Now display all the current drive settings.
MAP DISPLAY ON
MAP
```

Use the default login script only temporarily. The default login script is contained in the LOGIN.EXE file in SYS:LOGIN and cannot be edited.

Create a system login script before you create user login scripts. When planning login scripts, include as much as possible in the system login script. The more the system login script accomplishes, the shorter user login scripts can be.

If you access the box for a user login script in SYSCON and put in a blank space, the system thinks a user login script exists and stops the user from accessing the default login script.

If you want to execute a system login script and do not want to create a login script for every user, do one of the following:

- **Place the EXIT command at the end of the system login script.** This causes login script processing to end before checking for the user login script. No user login scripts can execute.
- **Use the script option of the LOGIN command.** This option executes a file containing valid commands. It does not use the system, user, or default login scripts. Since the login script attaches before executing the script option, the file can be located on the network. The following command executes only the system login script for most users:

#LOGIN /S SYS:PUBLIC\NET$LOG.DAT↓

Other users could remove the /S option and have their own login scripts.

For more information and examples, see Login scripts in *Concepts* and "Plan the login scripts."

The following commands can be used in login scripts:

(Executes a valid .COM or .EXE file.)

ATTACH

BREAK

COMSPEC

DISPLAY

DOS BREAK

DOS SET

DOS VERIFY

DRIVE

EXIT

FDISPLAY

FIRE PHASERS

GOTO

IF...THEN...ELSE

INCLUDE

MACHINE

MAP

PAUSE

PCCOMPATIBLE

REMARK

SHIFT

WRITE

The following identifier variables can be used with login commands such as IF...THEN, MAP, or WRITE.

Identifier Variable	Screen Display
CONDITIONAL	
ACCESS_SERVER	Returns TRUE if Access Server is Functional; otherwise, FALSE
ERROR_LEVEL	An Error Number, 0 = No Errors
MEMBER of "group"	Returns TRUE if member of group; otherwise, FALSE
DATE	
DAY	Day number (10–31)
DAY_OF_WEEK	Day of week (Monday, Tuesday,)
MONTH	Month number (01 – 12)
MONTH_NAME	Month name (January, June)
NDAY_OF_WEEK	Weekday number (1 – 7, Sunday = 1)
SHORT_YEAR	Year in shorter format (93, 94)
YEAR	Year in full format (1993, 1994)
DOS ENVIRONMENT	
< >	Use any DOS environment variable as s string

Identifier Variable	Screen Display
NETWORK	
NETWORK_ADDRESS	Network number of the cabling system (& hex digits)
FILE_SERVER	Name of the file server
TIME	
AM_PM	Day or night (am or pm)
GREETING_TIME	Morning, afternoon, or evening
HOUR	Hour of day or night (1 – 12)
$HOUR_{24}$	Hour (00 – 23, midnight = 00)
MINUTE	minute (00 – 59)
SECOND	Second (00 – 59)
USER	
FULL–NAME	User's full name (from SYSCON files)
LOGIN_NAME	User's unique login name
USER_ID	Number assigned to each user
WORKSTATION	
MACHINE	The machine the shell has written for (for example, IBMPC)
OS	The workstation's operating system (for example, MSDOS)
OS_VERSION	The version of the workstation's DOS
P_STATION	Station address of node address (12 hex digits)
SMACHINE	Short machine name (for example, IBM)
STATION	Connection number

Each login script command is explained in this section. The commands appear in alphabetical order.

A few conventions apply to creating login scripts:

- Command lines cannot exceed 150 characters.
- Allow long commands to wrap to the next line if there is not enough room on one line.
- Only one command can be entered on each line. The command interpreter reads the script one line at a time. Press **<Enter>** at the end of each command.
- Commands can be entered in either upper– or lowercase letters. Identifier variables enclosed in quotation marks must be preceded by a percent sign (%) and typed in uppercase letters.
- Comments can be included after any command except ATTACH, COMSPEC, DISPLAY, FDISPLAY, DOS SET, EXIT, MACHINE, MAP, and WRITE. Any text is considered a comment if it is preceded by an asterisk (*) or a semicolon (;).
- All variables except the conditional variables can be used with any login script command that uses a parameter, as long as the value returned by the variable falls within the limits expected by the command. Use conditional variables only with the IF...THEN command.

For instructions on accessing the entry box for login scripts, see **SYSCON** in *Utilities*.

(Executes a valid .COM or .EXE file.)

Use EXTERNAL PROGRAM EXECUTION (#) to execute a command that is external to the login script.

Command format

[*path*] *filename parameter line*

Replace *path* with a full directory path beginning with a DOS drive letter or a NetWare volume name.

Replace *filename* with an executable file (.EXE or .COM) excluding the extension.

Replace *parameter line* with any parameters that must accompany the executable file.

How to use

If you want the LOGIN utility to execute a command that is external to the login script, enter in the script a command line similar to the following:

#COMMAND /c BATCHFILE ↵

NOTE: You can execute batch files from the login script by typing a command similar to the one above.

The following restrictions apply:

- The COMSPEC variable in the workstation's DOS environment must specify the location of COMMAND.COM.
- When you specify the batch file name, do not specify a path; instead, have a search drive mapped to the path where the batch file is located.

The following restrictions apply:

- The command statement must appear on its own line.
- The first character on the script line must be a pound sign (#).
- The command should appear after MAP assignments, because the program will execute in the environment of drive mappings, default drives, and search drives set up previously in the login script.

This command function will fail if the given directory is invalid, if proper security rights are lacking, if the execute file cannot be found, or if there is insufficient workstation memory to load the execute file.

The login script is held in memory when the # command is run. The login script is not released from memory until you return to the script and either complete or exit the script.

Example

Suppose user Chris wants to use the CAPTURE command to print to a printer on server "Bottleneck" on the print queue "Mary_HP" for an application not designed to print to a network queue. She also wants the following capabilities: to print without exiting the program, with no form feed, and with no banner. She would enter the following command in her login script:

#CAPTURE S=bottleneck Q=mary_hp TI=5 NFF NB ↵

(For an explanation of CAPTURE and the symbols in the above example, see **CAPTURE** in *Utilities*.)

ATTACH

Use ATTACH to connect to additional file servers without interrupting the current execution of the login script.

Command format

ATTACH [*fileserver* [*/username* [*;password*]]]

How to use ATTACH

Enter this command in your login script:

ATTACH

You can also specify a file server, a username, and a password.

If you use the ATTACH command without supplying the above–mentioned variables, you are prompted to enter them when you log in. The following prompts appear (one at a time) on your screen:

```
Server:
Username:
Password:
```

You are prompted to enter only those variables that you have not included. For example, if you enter ATTACH and the name of the file server in your login script, you are prompted to enter only your login name and password for that file server.

NOTE: Be careful about including passwords with the ATTACH command. Security is at risk if others can find passwords to file servers that they normally are not allowed to access.

If you use other file servers infrequently, use the command line utility ATTACH. Attaching to file servers from a login script

uses up an extra connection slot on the file server and takes extra memory.

NOTE: You can attach to as many as eight file servers, including the one that you logged in to.

If you attach to several file servers regularly, we recommend that you use the same username and password on each file server (unless you attach as GUEST, since GUEST usually does not require a password). In this case, the command ATTACH FS2 attaches your workstation to FS2 and logs you in using the username and password you specified when you logged in to the default file server.

Using the same username and password enables you to attach without having to include your password. If you were already logged in to file server FS1, your attach command would be similar to the following:

ATTACH FS2

However, even if you use different usernames and passwords for different file servers, you can still place the ATTACH command in your login script. The login program prompts you to enter the username and password (if a password is required) for the file server you are attaching to.

By using the same username and password on several file servers and attaching to them in your login script, you gain an additional advantage. If your password expires on any of the servers, the login program lets you enter a new password and synchronize your password on all other file servers you have a username and a password for.

Example

To attach to file server FS2 as user FRED (whose password is "Music"), add the following to the login script:

ATTACH FS2/FRED;MUSIC↵

BREAK

BREAK ON allows you to terminate the execution of your login script. The default is BREAK OFF.

Command format

BREAK ON | OFF

How to use BREAK

If BREAK ON is in your login script, you can press **<Ctrl–C>** or **<Ctrl><Break>** to abort the normal execution of your login script.

Including BREAK ON in your login script does not affect the DOS **<Ctrl><Break>** check.

When the BREAK option is ON, type–ahead keyboard input is not saved in the buffer. If you find this side effect undesirable, leave the break option in its default form, BREAK OFF.

COMSPEC

Use COMSPEC to specify the directory that DOS uses to reload the command processor.

Command format

COMSPEC = [*path*] *filename*

Replace *path* with the directory path beginning with a DOS drive letter or a NetWare volume name.

Replace *filename* with COMMAND.COM (in most cases).

How to use COMSPEC

If more than one version of DOS is available on your network, a directory will have been created for each DOS version. The COMSPEC command must be used to reload the proper COMMAND.COM (the command interpreter file) for the computer and operating system each user is using.

To specify the location (directory or drive) from which the program is loaded, enter the appropriate version of the COMSPEC command in your login script. The *filename* is usually COMMAND.COM. If you are using a specially modified command processor instead of COMMAND.COM, replace *filename* with the name of your command processor. No more than 12 characters can follow the drive specification.

This command modifies the environment variable "COMSPEC" that is set in the AUTOEXEC.BAT file.

Examples

The following commands load COMMAND.COM from the third network drive:

```
MAP *3=SYS:PUBLIC\%MACHINE\%OS_VERSION
COMSPEC=*3:COMMAND.COM
```

The following loads COMMAND.COM from a local drive:

```
COMSPEC=C:COMMAND.COM
```

The following loads COMMAND.COM from a search drive:

```
MAP S16:=SYS:DOS\%MACHINE\%OS_VERSION
COMSPEC=S16:COMMAND.COM
```

The following loads COMMAND.COM from a fake root directory when the script command is interpreted:

```
MAP ROOT D:=SYS:DOS\%MACHINE\%OS_VERSION
COMSPEC=D:COMMAND.COM
```

DISPLAY

Use DISPLAY to show the contents of a specified text file on your workstation screen during the login.

Command format

DISPLAY [*path/*] *filename*

How to use DISPLAY

To instruct the operating system to display a certain file for you when you log in, enter the following command, replacing the variables (*path* and *filename*) with the path name and the name of the file you want to see when you log in:

DISPLAY [*path/*] *filename*

The exact characters contained in the file, including "garbage" such as printer and word processing codes, appear on your workstation screen. See FDISPLAY for contrasts.

Example

Suppose you put messages in a public "bulletin board" file (SYS:PUBLIC/MESSAGES/SYSNEWS.TXT, in this example) and you want members of the SALES group to see this file when they log in.

To enable the operating system to display this file automatically, you can type a command similar to the following in the system login script:

IF MEMBER OF "GROUP" THEN

DISPLAY SYS:PUBLIC/MESSAGES/SYSNEWS.TXT

If the DISPLAY command is in the system login script, any messages you put in the file appear on the users' screens when

they log in. For example, if you update the SYSNEWS.TXT file with the message, "Meeting for everyone Tuesday at 2:00," users receive the message when they log in. (If the given directory does not exist or if the given file is not found, no error message appears on the users' screens when users log in.)

DOS BREAK

Use DOS BREAK to set the <**Ctrl**><**Break**> checking level for DOS. If the DOS BREAK command is set to ON, whenever a program sends a request to DOS, you can terminate program execution with <**Ctrl**><**Break**>. (This command is different from the BREAK command that terminates the login script.)

Command format

DOS BREAK [ON | OFF]

How to use DOS BREAK

Enter the following command in your login script:

DOS BREAK ON

The default is DOS BREAK OFF. For more information, see the BREAK command in your DOS manual.

DOS SET

Use DOS SET to set a variable in a DOS environment to the specified value.

Command format

[*option*] [DOS] **SET** *name* = "value"

Replace *option* with the keywords LOCAL, TEMP, or TEMPORARY. This sets the variable only in the environment of the login script, not in the PC environment.

Replace *name* with an environment parameter that identifies the environment you want to change.

Replace *value* with identifier variable substitutions.

For more information about identifier variables, refer to "Identifier variables" for the IF...THEN...ELSE command.

How to use DOS SET

The DOS SET login script command is similar to the DOS command called SET. However, the DOS SET login script command requires you to enter double quotation marks (" ") around values, while the DOS command SET does not. To give a variable name whatever value you specify, place the following in your login script:

DOS SET *name* = *"value"*

For information about values you can set, see the SET command in your DOS manual.

Example 1

The following sets your prompt to show your directory path:

SET PROMPT = "PG"

SET PROMPT lists your directory path at the DOS prompt rather than just the drive letter. $P lists the directory; $G provides an ">" character. See your DOS manual for more information.

Example 2

To remove a variable from the DOS environment, leave the command line blank after the equal sign:

DOS SET *name* =

or

SET *name* =

NOTE: Since DOS environments have a fixed maximum size, this command cannot work if your environment is too small. To increase the environment size, type **SHELL=COMMAND.COM /E:200 /P** in the CONFIG.SYS file. This command increases the environment size from 127 to 200 bytes (if you are using DOS 3.2 or above). For more information about environment size, see the SHELL command in your DOS manual.

Example 3

Use double backslashes to set a path for a program:

SET DLYPATH = "G:\\REPORTS\\DAILY"

This sets the variable DLYPATH to G:\reports\daily.

NOTE: The backslash is used as a special programming character in NetWare commands; it is not recognized

as a normal backslash unless you enter two backslashes.

Example 4

To increment numbers for looping, type

SET X = "1"

SET X = <X> + "1"

This adds one to the variable *x*. See GOTO for an example of how to use looping.

DOS VERIFY

Use DOS VERIFY to verify that data copied to a local drive can be read without an error. The default is OFF.

Command format

DOS VERIFY [ON | OFF]

How to use DOS VERIFY

The DOS COPY command, unlike the NetWare copy command (NCOPY), does not automatically verify that data copied to a local drive can be read after the copy. If you want DOS to make the same verification, you must enter the DOS VERIFY ON command in your login script. This command may not work with some software that is copy–protected.

If you have not entered a DOS VERIFY ON command in your login script but still want a particular copy verified, you must add the /v option to the DOS COPY command, as in the following example:

COPY *filename* **to** *local drive*: **/v**

In other words, if you want to make sure that data copied to a local drive has been copied correctly, you can do any of the following:

- Enter the DOS VERIFY ON command in your login script.
- Use the NCOPY command.
- Add the /v option to the DOS COPY command.

DRIVE

You can use DRIVE to specify which drive is your default drive.

Command format

DRIVE [*d*: | **n*:]

Replace *d* with a local or network drive letter.

Replace *n* with a drive number.

How to use DRIVE

Unless you have entered this command in your login script, your default drive is set to the first network drive, which is often assigned to your home directory when you log in.

Enter the DRIVE command in your login script, replacing *d* with the appropriate drive. For example, the following specifies drive J as your default drive:

DRIVE J:

The drive you specify must be defined in your login script in a separate MAP command entered on any line above the DRIVE command entry.

Example

Suppose you expect to be working on only one project for several days and the information for the project is located on drive S. You can use the DRIVE command to set your default drive to S (so you won't have to change the drive specification manually every time you log in).

DRIVE S:

EXIT

Use EXIT once per login script to terminate execution of the LOGIN utility and to execute one .COM, .EXE, or .BAT file, or one DOS internal command, such as DIR.

Command format

EXIT [*"filename"*]

How to use EXIT

The following command in your login script terminates the login utility:

EXIT

Caution: Any login script command entered on any line below the EXIT command is ignored.

You can use the EXIT command to pass a short command to COMMAND.COM (the command interpreter for the operating system you are using). The command is placed in the type–ahead buffer. If you have added a long machine name in SHELL.CFG or NET.CFG, use the PCCOMPATIBLE command on the line above for the short command to work. The short command following the EXIT command cannot exceed 14 characters:

EXIT *"filename"*

Caution: Do not use the EXIT command in your login script to exit to a terminate–and–stay resident (TSR) program (such as SideKick or any terminal emulator that terminates and stays resident).

The EXIT login script command is available only on IBM PCs and compatibles, unless you use the PCCOMPATIBLE login script command.

Example 1

If you don't want to create individual login scripts and don't want the default login script to execute, enter the following at the end of the system login script:

EXIT

Example 2

If your long machine name is IBM_PC (the default) and you want to exit to a menu program, enter the following at the end of the login script:

EXIT "MENU"

Example 3

If you have a Hewlett–Packard computer and you have changed the long machine name to HE_PAC in either the SHELL.CFG or the NET.CFG file, the following exits to a menu program at the end of the login script:

PCCOMPATIBLE

EXIT "MENU"

Example 4

If you want to exit the LOGIN utility to the electronic mail system (EMAIL, for example), type the following IF...THEN statement in your login script.

IF "%2" = "EMAIL" THEN EXIT "EMAIL"

FDISPLAY

Use FDISPLAY to show the contents of a specified text file on your workstation screen during the login.

Command format

FDISPLAY [*directory/*] *filename*

How to use FDISPLAY

To instruct the operating system to display a certain file for you when you log in, enter the following command, replacing the variables (*directory* and *filename*) with the directory name and the name of the file you want to see when you log in:

FDISPLAY [*directory/*] *filename*

If you enter FDISPLAY, the text in the file is "filtered" and formatted so that only the text itself is displayed. FDISPLAY does not display tabs. See DISPLAY for contrasts.

Example

Suppose you put messages in a public "bulletin board" file (SYS:PUBLIC/MESSAGES/SYSNEWS.TXT, in this example) and you want members of the SALES group to see this file when they log in.

To enable the operating system to display this file automatically, you can place a command similar to the following in the system login script:

IF MEMBER OF "GROUP" THEN FDISPLAY SYS:PUBLIC/MESSAGES/SYSNEWS.TXT

If the FDISPLAY command is in the system login script, any messages you put in the file appear on the users' screens when

they log in. For example, if you update the SYSNEWS.TXT file with the message, "Meeting for everyone Tuesday at 2:00," users receive the message when they log in. (If the given directory does not exist or if the given file is not found, no error message appears on users' screens when they log in.)

FIRE PHASERS

Use the FIRE PHASERS command to alert you that certain conditions exist.

Command format

FIRE PHASERS *n* **TIMES**

How to use FIRE PHASERS

To fire phasers automatically, place the following in your login script:

FIRE PHASERS *n* **TIMES**

Replace *n* with the number of times (up to nine) that you want to hear this sound.

Example 1

The following executes the "phaser" sound four times when you log in:

FIRE PHASERS 4 TIMES

Example 2

Use this command with the IF...THEN command. You can specify that the sound will execute a different number of times depending on the circumstances of the login. For example, you could fire the phasers five times on Thursday by entering the following command:

IF DAY_OF_WEEK = "Thursday" THEN FIRE PHASERS 5 TIMES

or

FIRE PHASERS %NDAY_OF_WEEK TIMES

GOTO

Use GOTO when you want to execute a portion of the login script out of the regular sequence.

Command format

GOTO *label*

Use *label* to indicate where you want to continue executing the login script.

How to use GOTO

Do not use GOTO from within a BEGIN/END pair. For example, to execute a loop of commands, you could include the following:

```
SET X = "1"

LOOP:
SET X = <X> + "1"
;see compound strings for this
WRITE <X>
IF <X> IS LESS THAN VALUE "10" THEN GOTO LOOP
```

<X> is a DOS environment variable that is incremented with each loop.

Remember to allow IF commands to "wrap" to the next line if there is not enough room on one line.

Caution: *Set BREAK ON in your login script before experimenting with loops.*

IF...THEN...ELSE

Use IF...THEN...ELSE when you want login to perform commands conditionally, depending on whether specified conditions exist.

Command format

IF *conditional(s)* [**AND** | **OR** | **NOR**] *conditional(s)* **THEN** *command* **ELSE** *command*

How to use IF...THEN...ELSE

IF statements can be nested. The maximum nesting level is limited to 10. Sometimes you can embed two or more conditionals in one statement by using AND, OR, or NOR.

For example, if you have the following IF...THEN command in your login script, your workstation screen displays `"Welcome back!!"` when you log in on Mondays and `"Have a happy day!"` on other days.

IF DAY_OF_WEEK="Monday" THEN WRITE "Welcome back!!" ELSE WRITE "Have a happy day!"

The conditional is the statement that follows IF. In the example given above, DAY_OF_WEEK="Monday" is the conditional. Conditionals can be made with identifier variables, command line parameters, or DOS environment variables.

Identifier variables

The conditional can contain identifier variables that represent login information that varies depending on the circumstances, such as the date and time. In the example above, DAY_OF_WEEK is the identifier variable.

Any DOS environment variable can be accessed as an identifier by enclosing it in angle brackets. Identifier variables can be entered in either upper– or lowercase letters.

Some examples of conditionals made with identifier variables follow.

ERROR_LEVEL

Use the ERROR_LEVEL identifier variable as a conditional to execute a command only if certain conditions are met. ERROR_LEVEL gives you control over error situations. If a command can be successfully executed, the error level is "0". If a command cannot be executed, the error level is represented by a value other than "0". You can use an 'If "ERROR_LEVEL"= "0" conditional to prevent the commands following the "THEN BEGIN" from being executed if an error occurs.

For example, if you normally need to access files on more than one file server, you could enter the following in your login script:

ATTACH *file server/username*
IF "%ERROR_LEVEL"="0" THEN MAP K:=*file server/volume:directory/subdirectory*

If the specified file server is down when you log in, an error level of "1" or some value other than "0" is returned, and the login program does not map a drive to that server. By using the ERROR_LEVEL identifier variable, you can avoid creating an error or receiving an error message.

ERROR_LEVEL searches for the last ATTACH or # (EXTERNAL PROGRAM EXECUTION) that was executed in the login script command. For example, if you attached to two file servers, it searches for the second ATTACH command.

The ERROR_LEVEL identifier is set after all commands that can fail. It is set to either the error level of the spawned process or the NetWare error code for internal login script commands.

NOTE: Allow IF commands to wrap to the next line if there is not enough room on one line.

Also, the ERROR_LEVEL identifier can be typed with an underscore (_) or as one word (ERRORLEVEL).

NETWORK_ADDRESS

Use the NETWORK_ADDRESS identifier to send a message to all users who are attached to the same cabling system.

For example, if you have intermittent error reports from users on a particular cabling system, you could send them a message similar to the following:

If NETWORK_ADDRESS = "00000ACC" write "Please report any problems with your workstation to Chris."

NOTE: The 3–digit cabling system number, ACC, is preceded by five zeros. Add zeros to all network addresses to make an 8–digit number when they are used in IF...THEN statements.

[NOT] MEMBER OF *"GROUP"*

The MEMBER OF *"GROUP"* identifier variable is similar to other conditionals but requires an "OF" rather than an "=" sign. It can be used like any other conditional in an IF statement. The MEMBER OF *"GROUP"* tests whether the user belongs to a certain group that you have defined on the

file server. For example, you might have the following command in a user's login script:

IF MEMBER OF "SALES" AND DAY_OF_WEEK = "MONDAY" THEN WRITE "Sales meeting at 10:00; BE THERE!"

If the user is a member of the group SALES and it is Monday, the user receives the message "`Sales meeting at 10:00; BE THERE!`" upon logging in.

Literal text (text that is not part of the command syntax) must be enclosed in double quotation marks (" "). For example, "Monday" and "Sales meeting at 10:00; BE THERE!" are both literal text; they will be displayed exactly as you type them. For more information on literal text, see WRITE.

P_STATION

Use P_STATION in an IF...THEN statement to send a message or perform operations on a specific workstation. For example, you could send a message similar to the following:

IF P_STATION = "000000001AB" then write "You need to update your workstation shell. Please see the system administrator."

NOTE: When you use P_STATION in an IF...THEN statement, capitalize P_STATION and make sure the station number is 12 digits long. If the network station address is a 3–digit number, precede it with nine zeros to make it a 12–digit number.

Command line parameters

You can use command line parameters in IF...THEN commands in your login script. When you log in, you can

specify parameters that the LOGIN command will pass to your login script.

When the login script is interpreted, any percent sign (%) entered in a command and followed by a number from 0 to 9 is replaced by the corresponding parameter from your LOGIN command line.

The file server name always corresponds to %0, and the login username always corresponds to %1. The next entry in the login command line corresponds to %2 in the login script, the next entry corresponds to %3, and so on. (The parameters %2 to %9 are variable.)

If you need more than 9 variables, use the SHIFT command to shift the %variable assigned to each command line parameter. For more information, see the SHIFT command.

You could include the following LOGIN command:

LOGIN COUNT/RON SALES MARKETING LEGAL

The server COUNT corresponds to %0 in the login script, the user RON corresponds to %1, the word SALES to %2, the word MARKETING to %3, and the word LEGAL to %4.

Remember that command line parameters are substituted in the script command. For example, IF "%0"="COUNT" would become IF "COUNT"="COUNT" as you log in.

Suppose that you want to log in to server COUNT every day and that sometimes you also want to attach to one or two other file servers on the internetwork. Type the following commands in your login script:

IF "%2" DOES NOT EQUAL "" ATTACH %2
IF "%3" DOES NOT EQUAL "" ATTACH %3

Then, when you log in, specify the additional file server (if any) that you want to attach to. For example, to log in to server

COUNT and attach to servers LEGAL and COMMS, include the following LOGIN command:

LOGIN COUNT/*username* LEGAL COMMS

To log in to server COUNT and attach only to server LEGAL, include

LOGIN COUNT/*username* LEGAL

To log in only to server COUNT, include

LOGIN COUNT/*username*

To attach to different file servers, substitute the server names for LEGAL and COMMS.

Relationships in conditionals

There are six possible relationships between the information contained in an IF...THEN statement: equal to, not equal to, greater than, less than, greater than or equal to, and less than or equal to.

You can represent equal and not equal relationships in the following ways:

Equal	Not Equal
IS	IS NOT
=	≠
=	< >
EQUALS	DOES NOT EQUAL NOT EQUAL TO

The other four relationships can be represented as follows:

>	IS GREATER THAN
<	IS LESS THAN
≧	IS GREATER THAN OR EQUAL TO
≦	IS LESS THAN OR EQUAL TO

The keyword VALUE has been added to force numeric rather than ASCII evaluations. In an ASCII evaluation, 10 is less than 5 because only the first integer, 1, is compared to 5. VALUE compares the total value of 10 to 5. For example,

IF VALUE HOUR24 >= "12" THEN WRITE "afternoon"

Conditionals can be joined with commas, the word AND, and the word OR to form compound conditionals. The following are compound conditionals:

IF GREETING_TIME IS "AFTERNOON" AND DAY IS "01"

(If it is the afternoon of the first day of the month)

IF HOUR24="23", MINUTE="59", AND SECOND="59"

(If it is 11:59:59 p.m.)

Entering login script commands after THEN

The command following the THEN can be a single statement or the beginning of a block of commands. The statement or block of commands is interpreted only if all of the specified conditions are true.

Single statement

The following is an example of a single statement:

IF NDAY_OF_WEEK="6" THEN

WRITE "HOORAY! IT'S FRIDAY!"

Block of commands

You must start a block of commands by specifying BEGIN or DO after the THEN in the IF...THEN statement. BEGIN or DO must be entered on the same line as the conditional IF. When you have entered all the conditional commands you want, end the block by specifying END.

For example, type this IF...THEN statement:

IF DAY_OF_WEEK="Tuesday" THEN BEGIN
WRITE "Staff meeting today at 10 a.m."
INCLUDE SYS:PUBLIC/UPDATE
END

In this case, on Tuesdays you receive the message about staff meeting. Your login script also processes any commands or messages contained in the file SYS:PUBLIC/UPDATE.

INCLUDE

Use INCLUDE to create the login script interpreter process "subscripts" that are not contained in the login script being processed. These subscripts are text files that contain valid script commands (any of the commands explained in this section).

Command format

INCLUDE [*path*] *filename*

Replace *path* with the directory path to a specific file.

Replace *filename* with the text file to include as a subscript in the login script.

How to use INCLUDE

You can create and edit subscripts using any text editor or word processor.

NOTE: INCLUDE nesting is limited only by memory. This means that one script file can INCLUDE another script file which, in turn, can INCLUDE yet another script file, and so on. You must have at least File Scan and Read rights in any directory containing a subscript you want to use.

Example 1

Suppose you want to allow workgroup managers to create a subscript containing different commands for users in the workgroup manager's group. Place the following statements in the system login script:

IF MEMBER OF "SALES" THEN INCLUDE SYS:MANAGERS\SALES.LOG

IF MEMBER OF "ACCTNG" THEN INCLUDE SYS:MANAGERS\ACCTNG.LOG

NOTE: The INCLUDE command does not function in the same way as the DISPLAY or FDISPLAY commands. In order for it to display text as shown in this example, the included file must contain WRITE commands.

Example 2

The INCLUDE command can also be used to shorten users' login scripts. You may want to create one script file and then have each user who needs it include the script file in his or her login script with the INCLUDE command, instead of having the user type the extra commands in the script. To do this, the user could include the following line in the login script:

INCLUDE MAIL.SCN

MACHINE

Use MACHINE to set the machine name of the station to the specified name.

Command format

MACHINE = *"name"*

How to use MACHINE

The machine name can contain up to 8 characters. (Longer machine names will be set to the default of IBM_PC.)

The MACHINE command is necessary for some programs (such as NETBIOS) written to run under PC–DOS. The name can include such identifier variables as %STATION. For more information about identifier variables, see "Identifier variables."

MAP

Use MAP to map a drive to a directory on the network. Before you can work in a network directory, you must have a drive mapped to that directory.

NOTE: You cannot map a drive to the root of a NetWare volume on a host directory structure.

Command format

MAP [*option*] [*drive*:= [*path*[;;;;] [*variable*]]

Command options

Replace *option* with one of the following commands. For more information on these commands, refer to them in the remainder of this section.

DISPLAY ON/OFF

ROOT

ERRORS ON/OFF

INS

DEL

Replace *drive* with any valid network, local, or search drive.

Replace *path* with a full directory path beginning with a DOS drive letter or NetWare volume name.

Add additional mappings to the same line by separating them with a semicolon.

Replace *variable* with one of the following identifier variables:

OS	The workstation's operating system (e.g., MSDOS)
OS_VERSION	The version of DOS (e.g., 3.30)
MACHINE	The long–machine name assigned in SHELL.CFG or NET.CFG
SMACHINE	The short–machine name assigned in SHELL.CFG or NET.CFG

For information on SHELL.CFG see "SHELL.CFG Options." For information on NET.CFG see "NET.CFG Options."

Variations of the MAP command

The headings which follow show the various command formats of the MAP command.

MAP

Displays the current drive mappings for all drives on the workstation. Undefined local drives (drives that have not been mapped to a directory) will not be displayed.

MAP *drive:=directory*

Maps the specified drive to the given directory. *Directory* refers to the directory path, beginning with the volume name.

MAP *drive:=directory; drive:=directory ...*

Maps multiple drives to multiple directories with one command. This command has the same result as executing the command MAP *drive:=directory* two or more times.

Directory refers to the directory path, beginning with the volume name.

MAP *drive:=drive:*

Maps the first drive to the same directory that the second drive is mapped to.

MAP DISPLAY OFF

Does not display your drive mappings when you log in.

MAP DISPLAY ON

Displays your drive mappings when you log in. This is the default setting.

MAP ERRORS OFF

Does not display MAP error messages.

You can use MAP DISPLAY ON and MAP DISPLAY OFF anywhere in your login script; however, you must place MAP ERRORS ON and MAP ERRORS OFF before the drive mappings in your login script.

MAP ERRORS ON

Displays MAP error messages (messages that report serious errors encountered while mapping drive assignments). This is the default setting.

MAP INSERT *search drive:=directory*

Inserts a new search drive using the next available letter in the search drive sequence. *Directory* refers to the directory path, beginning with the volume name.

MAP ROOT *drive:=directory; drive:=drive*

Maps a drive to a fake root directory. Some software applications write files to and read files from the root directory only. Because users do not have rights in the root directory, they cannot retrieve or write to files they create in those applications. NetWare allows users to map a drive to a fake root directory in which they have the rights they need.

How to use MAP

When you use MAP to save drive mappings in your login script, you don't have to remap drives to directories every time you log in. This command is especially useful if you frequently use a number of directories and don't want to specify drive mappings for them every time you log in.

You can specify drive mappings in your login script by entering the same commands that you would enter if you were using the regular MAP command at the command line. These mappings will be displayed when you log in, unless you have entered MAP DISPLAY OFF in your login script.

Your workstation has 26 logical drives (assigned letters A through Z) that you can use to map to directories in all areas of the network directory structure. Some of these logical drives will be assigned to local drives when you log in. Up to 16 of the 26 drives can be assigned as search drives.

When specifying drive names such as F or G, you can use an asterisk followed by a number *n* to represent the *n*th network drive.

For example, if your workstation has two local drives, A and B, then *1: maps to one of two drives: either the first drive beyond the drive specified by the LASTDRIVE command found

in the CONFIG.SYS configuration file (see the DOS manual) or drive F if no LASTDRIVE command is used. It is generally best to use the relative specification *n:; this allows you to log in from workstations with different local drive configurations.

NOTE: DOS 3.0 and above generally assigns five local drives by default. You can override the default by using the LASTDRIVE command in your DOS CONFIG.SYS file.

You can map a local drive to a network directory, but you will not be able to access the local drive until you remove the network drive mapping. You can initially assign *1: to a user's home directory. Users can redefine *1: if they choose.

NetWare handles search drives differently. If you map a search drive with a number that hasn't been used, NetWare will assign the search drive to the next available number.

For example, if you had three search drives mapped and mapped S7: to an application directory, NetWare would assign it as S4:.

If you map a search drive using a number already assigned to a search drive, NetWare makes the old search drive a network drive.

If you use the insert option to map a search drive to Z:, NetWare moves the old Z: search drive to Y:, Y: to X:, and so forth.

The easiest way to add a search drive is to enter the following:

MAP INS S16:= SYS:*PATHNAME*

NetWare will not disturb any existing search drives and will give the new search drive the next available letter.

Example 1

If you include the following map command in your login script, drive F is mapped to the SYS:SALES directory when you log in:

MAP F:=SYS:SALES

Example 2

If you include the following map command, your first network drive is mapped to the SYS:SALES directory when you log in:

MAP *1:=SYS:SALES; Q:=*1:TEST

Drive Q will be mapped to the subdirectory TEST relative to SYS:SALES (since you defined *1: to be mapped to the directory SYS:SALES).

Example 3

If you include the following map command, your next available search drive will be mapped to the SYS:WORDPROC directory:

MAP S16:=SYS:WORDPROC

Example 4

If you want to map a drive for the version of DOS assigned to each user in the system login script (or in each user's login script), it could appear as follows:

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

Make the mapped drive a search drive so that DOS commands can be accessed from any directory on the network.

The values for the identifiers come from the shell's descriptor area when the shell attaches to the file server during login.

Example 5

If you want to map a search drive to a user's DOS version without using the variables shown in Example 4, the assignment could appear as follows:

S2:=SYS:PUBLIC\HE_PAC\MSDOS\V4.00

The directory (indicated by the identifiers in the MAP command) should already exist and the correct DOS version should be loaded in the directory, or login will not complete successfully.

PAUSE

Use PAUSE to create a pause in the execution of the login script.

Command format

PAUSE

or

WAIT

How to use PAUSE

You can add PAUSE to the login script following a message so that you will have time to read the message before it scrolls off the screen. If you include PAUSE, the message `Strike a key when ready...` appears on the workstation screen. The login program then waits for a key to be pressed before it executes the rest of the login script.

Enter either of these commands in your login script at any point you want a pause to occur.

PAUSE

or

WAIT

PCCOMPATIBLE

Use PCCOMPATIBLE to include a filename with the EXIT login script command on all computers that are IBM PC compatible; you can also use it with computers that are not 100 percent IBM PC compatible.

Command format

[PC]COMPATIBLE

How to use PCCOMPATIBLE

If your machine is an IBM PC compatible but you have changed your long machine name in your SHELL.CFG file to another name (for example, HE_PAC, AT&T, or TANDY) to access a different version of DOS, you must use the PCCOMPATIBLE (or COMPATIBLE) login script command to inform the login program that your machine is an IBM PC compatible.

Place the following anywhere before EXIT in the login script:

PCCOMPATIBLE

For example, if you are working on an IBM PC compatible and you want to exit to SYSCON from within your login script, put the following commands in your login script:

PCCOMPATIBLE
EXIT "SYSCON"

REMARK

Use REMARK to insert explanatory text into your login script.

Command format

REM[ARK] [*text*]

or

* [*text*]

or

; [*text*]

How to use REMARK

Begin the line with REMARK (REM), an asterisk (*), or a semicolon (;). Any text that follows these symbols will be ignored when the LOGIN command interprets and executes your login script. The remark will not appear on your screen.

Using remarks in your login script can make the script much easier for you to read and understand.

The REMARK command and its associated text must be the only entry on a line. Placing remarks on the same line as other script commands will cause errors when your login script is interpreted.

To add explanatory text to your login script, include the following (or one of the other variants of the REMARK command) in your login script, entering the text you need in place of the *text* variable.

REMARK *text*

Example

The following are examples of explanatory text that you might use with the REMARK command:

```
* Craig's login script
; mapped network drives follow:
REM The mapping below does not work properly.
REMARK Starts mapping search drives here.
```

SHIFT

Use SHIFT to shift the command line arguments to the next variable. This allows you to enter command line arguments in any order. You can shift up to 10 arguments.

Command format

SHIFT [*n*]

Replace *n* with the number of places to the right you want the variable to shift. The default is 1.

How to use SHIFT

When you enter the LOGIN command, you can include additional arguments. These arguments are assigned a %variable.

In the login script, you can include a positive or negative number after SHIFT to move the variables in either direction. For example, "SHIFT –3" moves each %variable three positions to the left.

For example, Craig wants to log in to a word processing program, change the way it is set up, and map a drive to his work area called ACCNTS. Craig also has a command in his login script to map a drive to his LOTUS directory, but he does not need it today. Therefore, the commands in Craig's login script are as follows:

```
LOOP:

     IF "%2" = "WP" THEN SET WP="\U-CML\B-10\
        D-D\PS=Y:\APPL\WP\SETUP

     IF "%2" = "ACCNTS" THEN MAP G:=SYS:ACCNTS
```

```
    IF "%2" = "LOTUS" THEN MAP S16:=SYS:APPL\LOTUS

SHIFT 1
        IF "%2" <> " " THEN GOTO LOOP
```

With the preceding commands in his login script, Craig can log in as follows:

LOGIN FS1\CRAIG WP ACCNTS

The items of Craig's login command are given the following values:

%0 = FS1

%1 = CRAIG

%2 = WP

%3 = ACCNTS

Craig's login script looks for "%2" which is WP and sets the word processing environment. Then the login script shifts the variables one to the right so that "%2" now becomes ACCNTS. Upon executing the loop, the login script maps a drive to the ACCNTS directory.

Craig could change the order of his login command and do the following without harming the way his work environment is set up:

LOGIN CRAIG ACCNTS WP

The items of this login command are given the following values:

%0 = FS1

%1 = CRAIG

%2 = ACCNTS

%3 = WP

In this case, Craig's login script looks for "%2," which is now ACCNTS. The login script maps a drive to the ACCNTS directory. Then the login script shifts the variables to the right so that "%2" now becomes WP. Upon executing the loop, the login script sets the word processing environment.

WRITE

Use WRITE to customize your login messages.

Command format

WRITE ***"text"***

How to use WRITE

You can enter a single command or include a list of text strings or identifiers separated by semicolons (;) after any WRITE command. Each message appears on a new line on your screen unless you place a semicolon at the end of the WRITE command line. Then multiple WRITE commands generate a one–line display.

Text strings must be enclosed in double quotation marks (" ") and can include the following super–characters:

\r	for a carriage return
\n	for a new line
\"	for an embedded quotation mark
\7	to sound a beep

Compound strings

Compound strings are a general class of command arguments. A string is either a quoted sequence of characters or the value of an identifier (including the identifier variables listed on the following page). Strings can be combined into a single string using the following operators, highest precedence first:

;	Concatenation
* / %	Multiply, divide, modulo
+ –	Add, subtract
>> <<	Shift (truncate) left or right ("1000" >> 3 becomes "1")

The identifier variables on the previous chart can be used with login commands like IF...THEN, MAP, and WRITE. They can also be used with commands for which you can specify a path name, such as COMSPEC.

Actual values replace the identifier variables when the script line is interpreted.

The value of any environment variable set by DOS can be accessed as an identifier by enclosing it in angle brackets, as in the following examples:

```
WRITE "my path is %<path>"

IF <INCLUDE> != "" WRITE "my include path is ";<include>
```

Identifier variables can also be placed within literal text strings in a WRITE statement; however, the identifier name must be in uppercase letters and preceded by a percent sign.

For example, the following two lines would result in the same output:

```
WRITE "Good "; greeting_time; ", John"

WRITE "Good %GREETING_TIME, John"
```

NOTE: Identifier variables are extremely useful if you intend to use different PC operating systems concurrently on different network stations. Depending upon the operating system type, you can appropriately set search drive mappings and other OS–dependent mappings for the operating system you are using when you log in. Using identifier variables can provide a way to handle the different commands required by different machine types.

For example, if you are using PC–DOS 4.00, you could create a SYS:PUBLIC/IBM_PC/PCDOS/4.00

directory and place a copy of the appropriate COMMAND.COM in that directory. You could then create a similar directory for each different machine and operating system type. If your login script contained the following command, it would access the proper login command no matter which machine you execute LOGIN from:

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

Example

Suppose user Bill's login script contained the following WRITE commands:

WRITE "Hello, "; LOGIN_NAME

WRITE "This is station "; STATION

The following displays when Bill logs in to station 16:

```
Hello, BILL
This is station 16
```

Sample system login scripts

Following are three sample system login scripts. They may give you some ideas for your own system login script, or you could adapt them to your own situation.

Example 1

```
MAP DISPLAY OFF
MAP S1:=SYS:PUBLIC
MAP S2:=SYS:PUBLIC/%MACHINE/%OS/%OS_VERSION
MAP S3:=SYS:PUBLIC/APPLIC/WP
MAP S4:=SYS:PUBLIC/APPLIC/DB
MAP S5:=SYS:EMAIL/EXE
```

```
MAP S6:=SYS:EMAIL
MAP *1:=SYS:USERS/%LOGIN_NAME
MAP DISPLAY ON
MAP
WRITE
WRITE
WRITE "GOOD %GREETING_TIME, %LOGIN_NAME"
REM  IDENTIFIERS PLACED IN QUOTES MUST BE IN
REM  UPPER CASE WITH THE % PRECEDING THE
REM  IDENTIFIER
WRITE
WRITE
INCLUDE SYS:PUBLIC\SCRIPTS
PAUSE
WRITE
FDISPLAY SYS:SUPERVIS\MESSAGE
FIRE 4
PAUSE
PCCOMPATIBLE
EXIT "EMAIL"
```

EXIT in the system login script eliminates the need for all user login scripts.

Example 2

```
Write "Good %GREETING_TIME, %LOGIN_NAME."
MAP DISPLAY OFF
MAP ERRORS OFF
IF LOGIN_NAME <> "SUPERVISOR" THEN BEGIN
  MAP *1:=DC-2/SYS:HOME
  MAP *2:=DC-2/SYS:TRASH
  MAP *3:=DC-2/SYS:SYSTEM
```

```
  MAP *4:=DC-2/SYS:LOGIN
  MAP *5:=DC-2/SYS:PUBLIC
END
MAP S1:=DC-2/SYS:PUBLIC
MAP S2:=DC-2/SYS:PUBLIC\%OS_VERSION\%MACHINE
MAP S3:=DC-2/SYS:PUBLIC\TCP_OPT
COMSPEC=S2:COMMAND.COM
MAP DISPLAY ON
MAP
DOS SET USER=LOGIN_NAME
write " "
write "Type SSMENU to enter Support Services Menu."
write " "
write "If you wish to use the TCP Gateway, execute"
write "NETBIOS before entering the menu system."
```

Example 3

```
MAP DISPLAY OFF
MAP S1:=SERVER/SYS:PUBLIC;    S2:=S1:%MACHINE/%OS/%OS_VERSION
COMSPEC=S2:COMMAND.COM
MAP G:=SERVER/SYS:COMMON
MAP S16:=SERVER/SYS:APPS/DATABASE
MAP S16:=SERVER/SYS:APPS/SC4
MAP S16:=SERVER/SYS:APPS/WP
MAP S16:=SERVER/SYS:ATC/EXE
#CAPTURE NB NFF TI=30
DOS VERIFY ON
SET PROMPT = "$P$G"
MAP F:=SERVER/VOL1:USERS/%LOGIN_NAME
IF MEMBER OF "ACCT" THEN BEGIN
MAP INS S3:=SERVER/SYS:ACCTING
END
```

```
PCCOMPATIBLE
EXIT "MENU DAILY"
```

NOTE: Remember to let long command lines in your login script wrap around.

Sample user login script

This is a sample of a user login script. It may give you ideas for your own login scripts, or you could adapt this one to your own situations.

Example

```
MAP G:=SYS:USERS\KAREN\WORKSPAC
MAP H:=SYS:USERS\COMPANY\LETTERS
#CAPTURE P=1 NB TI=10 NFF
IF DAY_OF_WEEK = "FRIDAY" THEN BEGIN
FIRE 9
WRITE "FRIDAY AGAIN:  GENERATE REPORTS"
MAP I:=SYS:APPLIC/DBB/REPGEN
END
SET PROMPT $P$G
EXIT "GOMENU"
REMARK GOMENU.BAT HAS MENU NAME
```

End of Appendix

B Installation Worksheets

The following pages contain blank and sample filled–in installation worksheets. We refer to these worksheets in other sections of this manual.

File Server Worksheet NetWare for AViiON Systems

AViiON File Server Name: _____
AViiON File Server Model: _____
Installed by: _____
NVT Server Name: _____
Internal Network Number: _____

SAP output file: _____
SAP error file: _____

	YES	NO
NVT active?	❑	❑
SPX active?	❑	❑
NetBIOS active?	❑	❑

Networks

LAN #	Network Number	Network Devices	Adapter Type	Frame/Packet Type
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				

AViiON File Server Name: the name by which this host is commonly known.

AViiON File Server Model: the model number, such as AV6200.

Installed by: your name

NVT Server Name: the hostname of the server that will serve NetWare Virtual Terminal clients. This is often the same name as your NetWare server, but it can also be another NetWare server name. You must supply a name even if you are not using NVT.

Internal Network Number: an 8–digit hexadecimal number by which this server is to be known on the NetWare network. If this is the only server on the network, you can keep the default value, ABCD1234. If there are other servers, the number must be unique. A suggested value is an approximate hex equivalent of the IP address of this host. For example, if the IP address is 128.221.209.250, you can create an Internal Network Number 80DDD1FA.

LAN #: A server can be connected to a number of different NetWare LANs. If you are connecting to one network, you need only complete one line, and the LAN # is 1.

Network Number: an 8–digit hexadecimal number that identifies the network you are joining. All servers in a given network specify the same number here.

Network Device: a device name identifying the type of network controller board or pseudo device the server uses for this network. The allowable types are: dgen0, hken0, inen0, cien0, vitr0, udp (for IP Tunneling). The device names are stored in the /dev directory in DG/UX.

Adapter Type/Frame Type

The Adapter Type is the type of adapter used in the network. This should match the type of adapter for the given device. Choices are ETHERNET_DLPI, TOKENRING_DLPI, and IP_TPI.

Frame/Packet Type:

The Frame Type specifies the type of packet header that the Ethernet or Token Ring driver should use. The default for Ethernet is ETHERNET_II, and the default for Token Ring is TOKEN–RING. The dfault for IP Tunneling is IP_UDP. The choices for this token are as follows:

Ethernet: ETHERNET_802.2,
ETHERNET_802.3,
ETHERNET_II, or
ETHERNET_0600.

Token Ring: TOKEN–RING

IP Tunneling: IP_UDP

The frame type you choose should match that used by other NetWare servers and clients on the network.

NVT active? yes if you want clients to be able to use NetWare virtual terminal.

SPX active? yes if you want to use RPRINTER and PSERVER printer utilities, and any other products that use SPX to work with NetWare, such as MHS for AViiON Systems.

NetBIOS active? yes if you plan to run NetBIOS–based applications.

SAP output file: the file name where you want to store status messages from Service Advertising Protocol.

SAP error file: the file name where you want to store error messages from Service Advertising Protocol.

NOTE: You can change any of the values you enter during the installation by running the SCONSOLE utility after you finish installing the software.

File Server Worksheet NetWare for AViION Systems

AViiON File Server Name: ACME
AViiON File Server Model: AV8000
Installed by:
NVT Server Name: ACME
Internal Network Number: 80DDF401

SAP output file: /dev/console
SAP error file: /dev/console

	YES	NO
NVT active?	☑	☐
SPX active?	☑	☐
NetBIOS active?	☑	☐

Networks

LAN #	Network Number	Network Devices	Adapter Type	Frame/Packet Type
1	80DDF4FF	/dev/hken0	ETHERNET-DLP1	ETHERNET_II
2	80DDF4FE	/dev/hken1	ETHERNET-DLP1	ETHERNET-802.3
3	80DDF4FD	/dev/vitr0	TOKEN_RING_DLP1	TOKEN_RING
4	80DDF4FC	/dev/udp	IP_TPI	IP_UDP
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				

Workstation Configuration Worksheet

Current workstation owner:_____ **Serial # :**_____
Network address for board A:_____ **Installed by:**_____
Network address for board B:_____ **Type of workstation:**_____

Floppy Diskette Drives:

A Drive:	B Drive:
❑ 5.25" 1.2MB	❑ 5.25" 1.2MB
❑ 5.25" 360KB	❑ 5.25" 360KB
❑ 3.5" 1.44MB	❑ 3.5" 1.44MB
❑ 3.5" 720KB	❑ 3.5" 720KB

Memory: Base:_____ Extended:_____ Expanded:_____ Total:_____
Internal hard disks:____ Memory:_____ Driver type:_____

Network board (Fill in columns that apply to each network board)

Name	Option number	I/O address	Memory address	Interrupt (RQ)	DMA channel	Station/Node address	Slot number

LAN driver

LAN A						
LAN B						

Boot information:
- ❑ Boot from hard disk
- ❑ Boot from diskette
- ❑ Boot by Remote Reset

DOS version:_____

Remote Reset checklist:
- ❑ Network board set to configuration option 0
- ❑ Remote Reset PROM(s) installed on LAN board
- ❑ Remote Reset enabled on network board

Remote boot filename:_____

Files needed to connect to the network:
- ❑ LSL.COM
- ❑ IPXODI.COM
- ❑ LAN driver
- ❑ Shell file NETX
  EMSNETX
  XMSNETX
  BNETX
  VLM
- ❑ NETBIOS.EXE and INT2F.COM
- ❑ Others_____
- ❑ NET.CFG options_____

Workstation Configuration Worksheet

Current workstation owner: Bill Jones Serial # : 123456789
Network address for board A: 02608C1B838 Installed by: SF
Network address for board B: _____ Type of workstation: 486

Floppy Diskette Drives:

A Drive:	B Drive:
☐ 5.25" 1.2MB	☐ 5.25" 1.2MB
☐ 5.25" 360KB	☐ 5.25" 360KB
☐ 3.5" 1.44MB	☐ 3.5" 1.44MB
☐ 3.5" 720KB	☐ 3.5" 720KB

Memory: Base: 640K Extended: 256K Expanded: _____ Total: 896K
Internal hard disks: _____ Memory: _____ Driver type: _____

Network board (Fill in columns that apply to each network board)

Name	Option number	I/O address	Memory address	Interrupt (RQ)	DMA channel	Station/Node address	Slot number
3C503		310	DC00	3	1	80DD1524	1

LAN driver

LAN A						
LAN B						

Boot information:
☑ Boot from hard disk
☐ Boot from diskette
☐ Boot by Remote Reset

DOS version: 5.0

Remote Reset checklist:
☐ Network board set to configuration option 0
☐ Remote Reset PROM(s) installed on LAN boar
☐ Remote Reset enabled on network board

Remote boot filename: _____

Files needed to connect to the network:
☑ LSL.COM
☑ IPXODI.COM
☑ LAN driver NETX
☑ Shell file EMSNETX
XMSNETX
BNETX
VLM

☑ NETBIOS.EXE and INT2F.COM
☐ Others _____
☐ NET.CFG options _____

Login Scripts Worksheet for File Server _____

System Login Script

rem *preliminary commands (optional)*

rem *greeting (optional)*

rem *display login message (optional)*

rem *attach to other file servers (optional)*

rem *NetWare utilities mappings*

MAP INS S1:=SYS:PUBLIC

rem *w DOS directory mapping and COMSPEC*

MAP INS S2 : =
COMSPEC = S2:COMMAND.COM

rem *application directory mappings*

rem *miscellaneous search drives (optional)*

rem *supervisor mappings*

rem *preliminary commands (optional)*

IF "%LOGIN_NAME" = "SUPERVISOR" THEN

rem *home or username directory mapping*

rem *work directory mapping (optional)*

rem *default printer mappings or printing batch files (optional)*

rem *display directory path at prompt*

SET PROMPT = "PG"

rem *display all current drive settings (optional)*

MAP DISPLAY ON
MAP

rem *run miscellaneous programs*

Basic User Login Script for_____ Group_____ Workgroup_____

rem *set environmental variables*

rem *individual drive mappings*

Basic User Login Script for_____ Group_____ Workgroup_____

rem *set environmental variables*

rem *individual drive mappings*

Login Scripts Worksheet for File Server _____

System Login Script

rem *preliminary commands (optional)*

MAP display off
BREAK OFF

rem *greeting (optional)*

Write "Good % GREETING.TIME,%LOGIN_NAME."
Write "You have logged in to acme from % station."

rem *display login message (optional)*

If member of "PAYCLERK" then write "Staff Mtg. Tues. 10 am"
FDISPLAY daily.msg
PAUSE

rem *attach to other file servers (optional)*

If member of "PAYCLERK" then attach HISTORY % LOGIN_NAME

rem *NetWare utilities mappings*

MAP INS S1 : = SYS:PUBLIC

rem *w DOS directory mapping and COMSPEC*

MAP INS S2 : =
COMSPEC = S2:COMMAND.COM

rem *application directory mappings*

IF MEMBER OF "ACCTING" THEN IF
MAP INS SIG : = APPS:SS

rem *miscellaneous search drives (optional)*

If member of "ACCTING" then MAP INS SIG : = APPS : SS

rem *supervisor mappings*

rem *preliminary commands (optional)*

IF "%LOGIN_NAME" = "SUPERVISOR" THEN

rem *home or username directory mapping*

MAP * 1 = SYS : % LOGIN_NAME

rem *work directory mapping (optional)*

rem *default printer mappings or printing batch files (optional)*

CAPTURE Q=2 TI=10

rem *display directory path at prompt*

SET PROMPT = "PG"

rem *display all current drive settings (optional)*

MAP DISPLAY ON
MAP

rem *run miscellaneous programs*

Basic User Login Script for_____ Group_____ Workgroup_____

rem *set environmental variables*

rem *individual drive mappings*

Basic User Login Script for_____ Group_____ Workgroup_____

rem *set environmental variables*

rem *individual drive mappings*

Directories Worksheet for File Server _____

Directory Structure					Files	File Attributes	Inherited Rights Mask	Directory Attributes
Volume:	Directory	/Subdirectory	/Subdirectory	/Subdirectory	(Source)		(Applies only to the contents of this directory)	(none automatically flagged)
SYS	*LOGIN*	*OS_2*			*login files (copied in at installation)*	*automatically flagged*	[S R W C E M F A]	
	MAIL	*subdirectory for each user created automatically*				*automatically flagged*	[S R W C E M F A]	
	SYSTEM	*subdirectory for queue/print server – automatically*			*system files (copied in at installation)*	*automatically flagged*	[S R W C E M F A]	
	PUBLIC				*public files (copied in at installation*	*automatically flagged*	[S R W C E M F A]	
	HOME	*user name created automatically if you use RDEF*			*user created*	*user defined*	[S]	
		Machine name	*DOS Directories* Operating system MSDOS	DOS version	*copies files from DOS diskettes*	[R F]	[S R W C E M F A]	

Directories Worksheet for File Server _____

Directory Structure					Files	File Attributes	Inherited Rights Mask	Directory Attributes
Volume:	Directory	/Subdirectory	/Subdirectory	/Subdirectory	(Source)		(Applies only to the contents of this directory)	(none automatically flagged)
SYS	*LOGIN*	*OS_2*			*login files (copied in at installation)*	*automatically flagged*	[S R W C E M F A]	
	MAIL	*subdirectory for each user created automatically*				*automatically flagged*	[S R W C E M F A]	
	SYSTEM	*subdirectory for queue/print server – automatically*			*system files (copied in at installation)*	*automatically flagged*	[S R W C E M F A]	
	PUBLIC				*public files (copied in at installation*	*automatically flagged*	[S R W C E M F A]	
	HOME	*user name created automatically if you use RDEF*			*user created*	*user defined*	[S]	
		Machine name	*DOS Directories* Operating system MSDOS	DOS version	*copies files from DOS diskettes*	[R F]	[S R W C E M F A]	
APPS	**WP**				**copied files from application diskette**			
	DBAPP				"			
DATA	**ACCTG**				**copied data files from backup**			
	PAY-ROLL				"			

Users Worksheet for File Server _____						Station Restrictions (Specify network and node address)	Managed by	Operator or Manager (Specify)
Full Name	Username	Used Application	Groups	Access to Directories (Specify)	Time Restrictions (If not default)			

Users Worksheet for File Server _____

Full Name	Username	Used Application	Groups	Access to Directories (Specify)	Time Restrictions (If not default)	Station Restrictions (Specify network and node address	Mngd. by	Oper. or Mgr. (Specify)
Susan R. Leiter	srleiter	WP						
Sue Ann Graves	sagraves	WP						
George Ellis	gellis	WP/dbapp						
Dan P. May	dpmay	database	payclerk	home:dpmay data:payroll	M-F 7am-6pm Sat 7am-1pm	1986 beef 2606C9F9696	sagraves	n/a
Judith L. Burns	jlburns	wp/dbapp						
Hal C. Rask	hcrask	wp/dbapp						
Jane M. Grady	jmgrady	wp/dbapp						
Sam H. Black	shblack	wp/dbapp						
Gamal H. Beltagi	ghbeltagi	wp/dbapp						
John A. Parker	japarker							

Group Worksheet for File Server _____ for Workgroup _____

Group Name	Basis of Group	Access to Directories	Trustee Directory Assignments	Access to Files	Trustee File Assignments
Full Name	Managed by				

Usernames of Members *(NetWare utilities list names alphabetically)*			

Group Worksheet for File Server _____ for Workgroup _____

Group Name	Basis of Group	Access to Directories	Trustee Directory Assignments	Access to Files	Trustee File Assignments
WPUSERS	**word processing**	**SYS: APPS:WP**	**[RF]**	**N/A**	**N/A**
Full Name	Managed by	**SYS:APPS:WP/SETUP**	**[RWCEMF]**	**N/A**	**N/A**
WordPerfect Users	**SAGraves**				
Usernames of Members *(NetWare Utilities list names alphabetically)*					
SRLEITER					
SAGRAVES					
GELLIS					
HCRASK					
JMGRADY					
SHBLACK					
GHBELTAGI					
JAPARKER					

User Defaults for File Server _____

☐ YES ☐ NO Account has expiration date?
Date account expires: _____

☐ YES ☐ NO Allow unlimited credit?
Low balance limit: _____

☐ YES ☐ NO Limit concurrent connections?
Maximum concurrent connections: _____

☐ YES ☐ NO Intruder Detection/Lockout?

Intruder Detection Threshold
(number of incorrect login attempts permitted): _____

Bad login count retention time
(how long after last incorrect login): Days ___ Hours ___ Min ___

☐ YES ☐ NO Lock account after detection? How long? Days ___ Hours ___ Min ___

☐ YES ☐ NO Require password?
Minimum password length: _____

☐ YES ☐ NO Force periodic password changes?
Days between forced changes? _____

☐ YES ☐ NO Limit grace logins?
Grace logins allowed: _____

☐ YES ☐ NO Require unique password?

Workgroup _____

☐ YES ☐ NO Install Accounting?

Inital Account Balance: _____

Time Restrictions	
SUN	
MON	
TUE	
WED	
THU	
FRI	
SAT	

User Defaults for File Server _____

☐ YES ☑ NO Account has expiration date?
Date account expires: _____

☑ YES ☐ NO Allow unlimited credit?
Low balance limit: _____

☐ YES ☑ NO Limit concurrent connections?
Maximum concurrent connections: _____

☐ YES ☐ NO Intruder Detection/Lockout?

Intruder Detection Threshold
(number of incorrect login attempts permitted): 3

Bad login count retention time
(how long after last incorrect login): Days 7 Hours ___ Min ___

☑ YES ☐ NO Lock account after detection? How long? Days 2 Hours ___ Min ___

☑ YES ☐ NO Require password?
Minimum password length: 5

☐ YES ☐ NO Force periodic password changes?
Days between forced changes? 40

☐ YES ☐ NO Limit grace logins?
Grace logins allowed: 6

☑ YES ☐ NO Require unique password?

Workgroup _____

☐ YES ☑ NO Install Accounting?

Inital Account Balance: _____

Time Restrictions	
SUN	
MON	
TUE	
WED	
THU	
FRI	
SAT	

Trustee Directory Security Worksheet for File Server _____

Directories (To be used in conjunction with Directories Worksheet) → user or group name	Trustee file Rights to be assigned to Groups or Individual Users (possible trustee rights: Supervisory, Read, Write, Create, Erase, File Scan, Access Control)						
	EVERYONE						
SYS:LOGIN	[ ]						
MAIL	automatically assigned [W C]						
SYSTEM	no rights						
PUBLIC	automatically assigned [R F]						
PUBLIC DOS Directories	[R F]						

Trustee Directory Security Worksheet for File Server _____

Directories (To be used in conjunction with Directories Worksheet) → User or group name	Trustee file Rights to be assigned to Groups or Individual Users (possible trustee rights: Supervisory, Read, Write, Create, Erase, File Scan, Access Control)						
	EVERYONE						
SYS:LOGIN	[ ]						
MAIL	automatically assigned [W C]	WPUSERS					
SYSTEM	no rights						
PUBLIC	automatically assigned [R F]						
PUBLIC DOS Directories	[R F]						
APPS:WP		[RF]					
APPS:WP:SETUP		[RF]					

Trustee File Security Worksheet for File Server _____

Use only if you need to redefine trustee rights for individual files		Trustee file Rights to be assigned to Groups or Individual Users (possible trustee rights: Supervisory, Read, Write, Create, Erase, File Scan, Access Control)					
USER OR GROUP NAME →							
Directory Path	*Filename*	EVERYONE	PAYCLERK				
SYS:LOGIN		*[ ]*					
MAIL		*automatically assigned [W C]*					
SYSTEM		*no rights*					
PUBLIC		*automatically assigned [R F]*					
SYS:LOGIMORACLE			*[RF]*				

Trustee File Security Worksheet for File Server _____

Use only if you need to redefine trustee rights for individual files		Trustee file Rights to be assigned to Groups or Individual Users (possible trustee rights: Supervisory, Read, Write, Create, Erase, File Scan, Access Control)					
USER OR GROUP NAME → Directory Path	*Filename*	EVERYONE	PAYCLERK				
SYS:LOGIN		[ ]					
MAIL		*automatically assigned [W C]*					
SYSTEM		*no rights*					
PUBLIC		*automatically assigned [R F]*					
SYS:LOGIMORACLE			[RF]				
SYS:LOGIMORACLE							

End of Appendix

C Installing NetWare for AViiON Systems on a Trusted DG/UX System

This appendix tells how to install NetWare for AViiON Systems software on a new or existing NetWare system and DG/UX Trusted system.

Before you install NetWare on a DG/UX Trusted system (also referred to as Trusted DG/UX), do the following:

- See the NetWare for AViiON Systems Transport and Services Release Notices for hardware and software prerequisites.
- Follow recommendations in Chapter 1.
- Have these manuals on hand to refer to:

  Trusted Facility Manual for the B1 Trusted DG/UX™ System (093–701114)

  Trusted Facility Manual for the C2 Trusted DG/UX™ System (093–701110)

  Audit System Administrators Guide for the B1 Trusted DG/UX™ System (093–701115)

  Audit System Administrators Guide for the C2 Trusted DG/UX™ System (093–701111)

Then complete the following tasks in order:

1. Create virtual disks and file systems for NetWare system files and user files.
2. Install the Transport software.
3. Optionally, install the Services software.
4. Reboot the AViiON server.
5. Finish up the installation by making all users hybrid users, and optionally, doing **pconfig** printer configuration procedures).

The sections that follow explain how to do these tasks.

Creating NetWare virtual disks and file systems

Follow procedures in the section "Creating NetWare virtual disks and file systems" in Chapter 2.

Installing the software

NetWare software consists of two packages: Transport and Services. You must install the Transport package. You can optionally install the Services package for NetWare services such as printing and filing services. With the Transport package alone, the server can provide client users access to other NetWare servers on the network.

NOTE: NetWare does not support server failover on Trusted DG/UX.

If you are not familiar with procedures for installing software packages in DG/UX, see the manual *Installing the DG/UX™ System* for details.

Installing Transport software on Trusted DG/UX

Follow these steps.

1. Log on as root. Make sure that all other users have logged off the system.

2. Take the system to run level 1. Type:

   init 1 ↵

3. Use **sysadm** to add the DG/UX group netware.

   From the **sysadm** Main menu, follow the menu path:

   8 User → 5 Group → 1 Add

   Use this information to answer the **sysadm** prompts:

   Group name: **netware**
   Group ID: **690**

   as indicated below.

   ```
   Group name: netware
   Group ID: 690
   Audit Mask:
   OK to perform operation?
   ```

4. Add the DG/UX user netware.

   From the **sysadm** Main menu, follow the menu path:

   8 User → 1 User Account → 1 Add

   Use this information to answer the **sysadm** prompts. (For **xxxx**, type your choice or accept the default.)

   User name: **netware**
   Model user name: **xxxxx**
   User ID:[51] **690**
   Password value: **xxxxx**
   Primary group name: [general] **netware**

```
Home directory: [/home/netware] /home/netware
User comment: xxxxx
```

as indicated below.

```
User name: netware
Model user name: xxxxx
Authentication ID: 53
User ID: [51] 690
Password value: xxxxx
Primary group name: [general] netware
Supplementary group name(s):
Home directory: [/home/netware] /home/netware
User comment: xxxxx
Shell program: [/sbin/sh]
Create home directory for "netware"? [no]
OK to perform operations? [yes]
```

Repeat Step 4. as needed to add other users.

5. Insert the NetWare Transport release media into the appropriate drive or device.

6. Use **sysadm** to install the Transport package. Type:

   asysadm installpackage ↵

7. Do one of the following:

- If you have not created group NetWare and user NetWare, the system displays the **sysadm** Main menu and prompts you to do so. Go to steps 3. and 4. for instructions on adding group NetWare and user NetWare. Then return to this step and continue the installation.
- If you have already created Group NetWare and User NetWare, accept the defaults as indicated below.

We recommend that you do not list file names while loading as this slows down the load.

```
Release Medium: [/dev/rmt/0]
Is /dev/rmt/0 ready? [yes]
NetWare 3.11/Transport of mm/dd/yy from Data General
Corporation
List file names while loading? [no]
Package name(s): [all]
OK to perform operation? [yes]

Loading NetWare 3.11/Transport of mm/dd/yy from Data
General Corporation.

Positioning the tape to load: nw_tran:prep

Preparing to load the packages....

Loading package nw_tran
Package nw_tran has been loaded.
Package load is finished.
The selected packages have been loaded.
Setting up nw_tran in usr.
Installing NetWare 3.11/Transport for AViiON Systems...
   Group netware already installed.
   User netware already installed.

Package nw_tran has been successfully set up in usr.
Setting up nw_tran in MY_HOST root.
```

8. Answer the **sysadm** prompts and accept the defaults at the remaining prompts, as indicated below. Your answers will look similar to the following examples:

```
Most of NetWare can be configured automatically, but
for a couple of items, such as server name, some input
is required.
NVT Host Name?: [acme] acme
Probing the network ....
Internal Network Number?: [80ddefe6] xxxxxxxx
Probing the network....
Changing llc_devices_ARG in /etc/dgux.params file
```

9. Use this information to choose the system name, and answer **N** at the server failover prompt.

NOTE: NetWare does not support server failover on Trusted DG/UX.

```
System Name?: [acme] acme
Install this NetWare server with Failover
support? [N]? N
```

Accept the defaults at the remaining prompts, as indicated below.

```
The NetWare transport needs to add items to the system
build files in order to complete the installation.
This step will verify that these items are properly
added before attempting to build the system.

System Name?: [acme] acme
Install this NetWare server with Failover
support? [N] N
Configuring system....
Building kernel....
```

... (The system pauses while building the kernel. Then the status message display continues)

```
Successfully built dgux.acme. Linked /dgux. You must
reboot in order for this kernel to take effect.
Installation of NetWare 3.11/Transport is complete.
Package nw_tran has been successfully set up in MY_HOST
root. Package setup for nw_tran is complete.
```

Procedures for installing the Transport software on Trusted DG/UX are now finished. If you are installing the Services software, continue the installation with the next section. Otherwise, continue with the section "Rebooting the Server."

Installing Services software on Trusted DG/UX

Follow procedures in the section "Installing the Services software" in Chapter 2.

Rebooting the server

Follow procedures in the section "Rebooting the server" in Chapter 2.

Finishing up

All users on a NetWare System installed on Trusted DG/UX *must* be hybrid users or they cannot log onto the system. If the following conditions occur, you must make all NetWare users hybrid users:

- After installing NetWare for AViiON Systems on Trusted DG/UX
- If you upgrade a DG/UX System running NetWare to Trusted DG/UX

To do so, first delete all current hybrid users, then add back all NetWare users as hybrid users, as described below.

Making all NetWare users hybrid users

Follow these steps.

1. Obtain a list of all NetWare users and all hybrid NetWare users on your system. Use these lists as checklists as you delete each current hybrid user
(in step 2), and then add back each NetWare user as a hybrid user (in step 3).

2. Delete all current hybrid users. To delete a hybrid user, follow the SCONSOLE main menu path:

```
2. Configuration →
2. Services Configuration →
3. Hybrid User Configuration →
3. Delete Hybrid User
```

   Answer screen prompts to delete a hybrid user. Repeat for all NetWare users.

3. Add back all NetWare users as hybrid users. To add a hybrid user, follow the SCONSOLE main menu path:

```
2. Configuration →
2. Services Configuration →
3. Hybrid User Configuration →
2. Add Hybrid User
```

Answer screen prompts to add a hybrid user. Repeat for all NetWare users.

Using audible events features

Once you install NetWare on a Trusted DG/UX System, you can use security features such as NetWare auditable events, the **audadmin** and **audprint** utilities, and system masks to monitor user activity. Below, we list system masks that send various types of NetWare auditable events to a DG/UX audit trail:

- NWAUDIT for all NetWare auditable events
- NWPRINT for printing auditable events. NWPRINT records printing events in the **pserver** and **rprinter** utilities.
- NWFILE for the following auditable events:

  in files – creating, renaming, opening, setting attributes, and erasing

  in directories – creating, renaming and deleting

These audible events features help you track user activity that might indicate security breaches. Refer to the Trusted DG/UX manuals (listed at the beginning of this appendix) for details on using these features.

IMPORTANT: If you change a regular DG/UX system with NetWare to a Trusted DG/UX System, you must also add NetWare audit

definitions to the system. To do so, re–install NetWare 3.11 Services for AViiON Systems.

Where to go from here

Once you finish making all NetWare users hybrid users, and reviewing available audible events features, do one of the following.

- If you have DG/UX printers (configured with **sysadm**) that you want to configure in your NetWare network, see the Chapter 2 section "Configuring DG/UX printers on NetWare with **pconfig**."
- Use the table on the next page to determine where to continue the NetWare network installation process.

If you need to	See
Install a DOS Workstation	*NetWare Requester for DOS*
Install an OS/2 workstation	*NetWare Requester for OS/2*
Install a MacIntosh workstation	*NetWare for MacIntosh Installation and Maintenance*
Install a router (bridge)	Chapter 3 – "Router Installation Management"
Install cabling	Installation supplements or documentation that ships with your network boards
Set up diskless workstations	*NetWare Requester for DOS*
Create users, directories, and network security	Chapter 4 – "Network File Services Setup"
Work with NetWare audits, **audadmin** or **audprint** utilities, or other features or procedures for NetWare on a Trusted DG/UX System	*Trusted Facility Manual for the B1 Trusted DG/UX™ System* (093–701114) *Audit System Administrator's Guide for the B1 Trusted DG/UX™ System* (093–701115) *Trusted Facility Manual for the C2 Trusted DG/UX™ System* (093–701110) *Audit System Administrator's Guide for the C2 Trusted DG/UX™ System* (093–701111)

End of Appendix

D Installing and Using High Availability Features with NetWare

This appendix describes two high availability methods, and tells how to install the server failover method on a NetWare system. This appendix includes information on:

- High availability methods: multi–path LAN I/O and NetWare server failover
- How NetWare server failover works
- Installing NetWare with server failover
- Modifying NetWare server failover with scripts
- Setting up NetWare to continue printing after failover

Read this appendix and sections on failover in *Managing the DG/UX System* and *Achieving High Availability on AViiON Systems* before you install NetWare with server failover.

For other types of NetWare installations, see:

- Chapter 2: To install NetWare for AViiON Systems (on a new or existing non–trusted DG/UX System)
- Appendix C: To install NetWare for AViiON Systems on a Trusted DG/UX system. (Trusted DG/UX does not support server failover.)

High availability methods

Two primary methods of implementing high availability features on DG/UX are:

- Multi–path LAN I/O
- Server failover (also called disk/system failover) for NetWare Transport and Services software

See *Achieving High Availability on AViiON Systems* for an overview of DG/UX high availability features.

Multi–path LAN I/O

When your DG/UX system is set up to use Multi–path LAN I/O, it has a redundant LAN controller configured within a single AViiON NetWare server. The redundant controller takes over if the primary controller or network should fail.

If a LAN controller failure occurs after you set up multi–path LAN I/O, no NetWare connections will be lost, as the secondary controller assumes the identity of the failed controller. NetWare users can continue as they normally would, with no interruption in services. See *Managing the DG/UX System* and *Achieving High Availability on AViiON Systems* for details on setting up your system for multi–path LAN I/O.

Server failover

When your NetWare system is set up to use NetWare server failover, it has a secondary system set up to take over if the primary system should fail.

While server failover has many high availability features, it is not fault tolerant, nor does it involve server mirroring. If a system failure occurs after you set up server failover, NetWare

connections are lost and NetWare services are temporarily interrupted while the secondary system takes over the disks managing Transport and Services functions. PC users receive a loss of connection error message.

However, NetWare services are restored as soon as the secondary system finishes taking over the disks and bringing up NetWare. NetWare users can then log back on and resume using NetWare as they normally would.

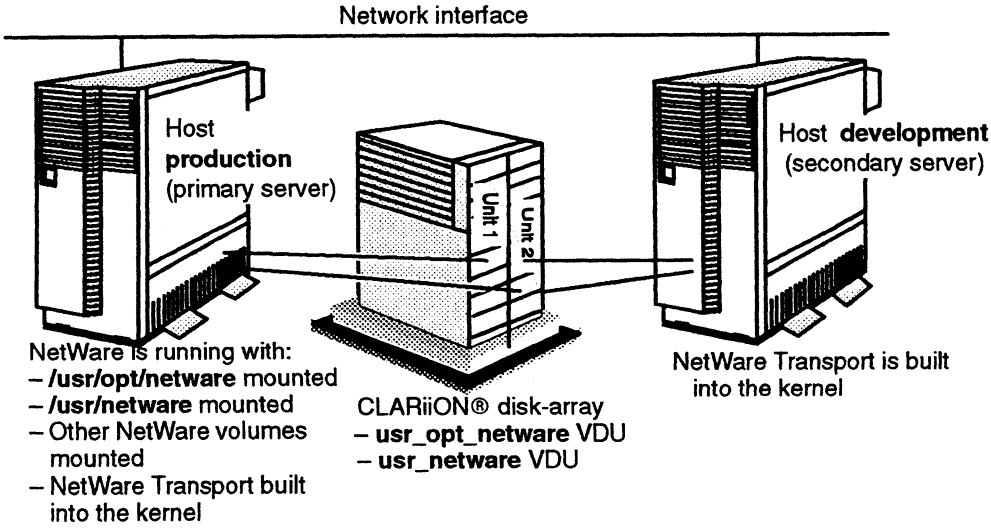
The rest of this appendix describes server failover concepts and processes.

How NetWare server failover works

This section describes what happens when a system failure occurs on NetWare system set up with server failover.

NOTE: This description assumes you set up server failover when installing the NetWare software (when the system automatically chose defaults for server failover features). If you want to modify the default process described here, see *Managing the DG/UX System* and *Achieving High Availability on AViiON Systems* for instructions on configuring failover disks, applications, and scripts. Also, see the later section "Modifying server failover with scripts."

This figure shows a NetWare system with server failover before a system failure occurs.



When a system failover occurs on a NetWare system set up with server failover, the following happens:

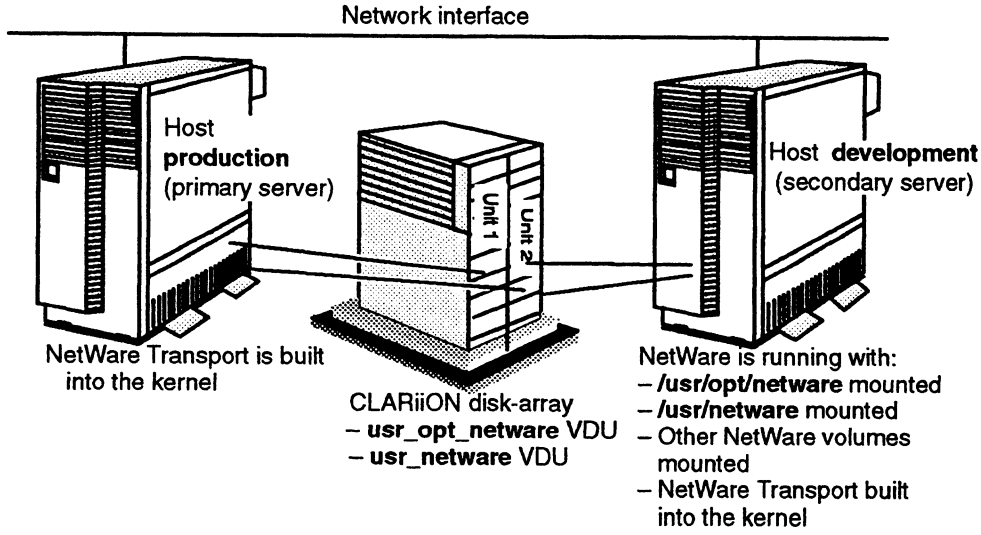
1. The secondary server detects (through the DG/UX failover monitor) that the primary server has failed.

2. The secondary system takes over the NetWare disks that you specified when you installed NetWare with server failover. These typically include disks containing the **usr_opt_netware** and **usr_netware** virtual disks and other disks that contain NetWare volumes.

NOTE: For machine–initiated failovers, the secondary system usually runs a file system check (**fsck**) on all the disks being switched over. This process can take several minutes.

3. The secondary server starts Transport software and, if installed, Services software.

This figure shows a NetWare system with server failover after a system failure occurs.



4. Once the primary server has come back up, the system administrator can decide when to use **sysadm** to switch the disk(s) and NetWare application back to the primary server. Because this process causes NetWare to come down, system administrators should do it at a time least disruptive for users.

Installing NetWare with server failover

This section tells how to install NetWare with server failover on a new or existing system.

If you have already installed NetWare, do not use the procedures in this section. Instead, set up server failover by running the **/usr/opt/netware/failover/nw_failover_setup** script on the primary server and the **/etc/failover/nw_failover_cleanup_secondary** script on the secondary server. See sections "Modifying server failover with scripts" and "Running nw_failover_cleanup_secondary" for details on these scripts.

To install NetWare with server failover, do the following tasks in order:

- Complete tasks in the section "Preparing to install NetWare with server failover."
- Install Transport software with server failover on the primary server.
- Optionally, for existing systems, run **nwbackup**.
- Install Services software with server failover on the primary server.
- Reboot the primary server.
- Install Transport software with server failover on the secondary server.
- Run **nw_failover_cleanup_secondary** on the secondary server.
- Reboot the secondary server.
- For existing systems, run **nwrestore**.

The sections that follow tell how to do these tasks.

Preparing to install NetWare with server failover

Do the following tasks before installing NetWare with server failover.

- Set up your DG/UX AViiON servers with server failover. Designate one server as primary and another server as secondary. See *Managing the DG/UX System* and *Achieving High Availability on AViiON Systems* for details on this task.
- Verify that the virtual disks you plan to set up are located on physical disks that can be switched over to the secondary server. See *Managing the DG/UX System* and *Achieving High Availability on AViiON Systems* for details on this task.
- Verify that TCP/IP communication exists between the primary and secondary server.
- Make sure that the server you plan to designate as a secondary host has not already been designated as a secondary server. If so, you cannot designate this server as the secondary server.

  Instead, you must add NetWare disks and startup scripts to the existing server failover setup. We provide sample scripts (in the **/usr/opt/netware/failover** directory) that show the startup scripts you must add to existing scripts. Your system creates these sample scripts when you answer **Y** at the prompt `Install this NetWare server with Failover support?` (or run the **nw_failover_setup** script), and specify a secondary server that is already defined on the primary server.

Installing NetWare with server failover

Follow these steps.

1. Verify that both the primary and secondary servers are at init level 3.

2. Verify that the primary server has remote copy access to the secondary server. See the **rcp** man page for instructions on this procedure.

3. Follow steps in section "Creating virtual disks and file systems" in Chapter 2, *but with the following requirement.* Locate the **usr_opt_netware** virtual disk and the **/usr/opt/netware** file system on a disk that both the primary and secondary servers can access.

4. If you plan to install Services software, follow steps in the section "Creating virtual disks and file systems" in Chapter 2, *but with the following requirement.* Locate the **usr_netware** virtual disk, the **/usr/netware** file system, and other virtual disks containing NetWare volumes on disks that both the primary and secondary servers can access.

Continue the installation with the next section.

Installing Transport software with failover on the primary server

Follow these steps.

1. If you are installing Transport software with server failover on a new system, follow *all but the last step* in the section "Installing the Transport software" in Chapter 2.

   If you are installing Transport software with server failover on an existing system, follow *all but the last step* in the section "Installing Transport over existing software" in Chapter 2.

   Then continue the server failover setup with the next step.

2. Answer the following **sysadm** prompts.

   ```
   System Name?: [production] production

   Install this NetWare server with Failover
   support? [N] Y

   Is this host the PRIMARY Failover Server?
   [Y] Y
   ```

   Answer **Y** to the server failover prompt and enter (or confirm) the host of the primary server. The NetWare setup scripts then display additional prompts and perform all the tasks necessary to set up your primary server for machine–initiated failover.

Accept the defaults at the remaining prompts, as indicated below.

```
   The NetWare transport needs to add items to the
   system build files in order to complete the
   installation.  This step will verify that these
   items are properly added before attempting to build
   the system.
   System Name?: [production] production
   Install this NetWare server with Failover support?
    [N]? Y
   Is this host the PRIMARY Failover
   server? [Y]? Y
   PRIMARY NetWare Failover system
Configuring system...
Building kernel...
Successfully built dgux.production.
Linked /dgux. You must reboot in order for this kernel
to take effect.
Installation of NetWare 3.11/Transport is complete.
Package nw_tran has been successfully set up in MY_HOST
root.
Package setup for nw_tran is complete.
```

If you are installing Services software, continue the installation with the next section. Otherwise, continue with the section "Rebooting the primary server."

Installing Services software with failover on the primary server

Follow these steps.

1. If you are installing Services software with server failover on a new system, follow *all but the last step* in the section "Installing the Services software" in Chapter 2.

   If you are installing Services software with server failover on an existing system, follow *all but the last step* in the section "Installing Services over existing software" in Chapter 2.

   NOTE: You must run **nwbackup** either before or during Services installation. See the section "Backing up existing file attributes and trustee rights" in Chapter 2 for instructions on running **nwbackup**.

   Then continue the server failover setup with the next step.

2. Specify the file server name and License Validation Key, and answer the server failover prompts.

   Use the following information to answer the **sysadm** prompts:

   `File Server Name` **production**

   The File Server Name is the name of the AViiON server on which you are installing the software. If the name of your system does not appear as the default, type the correct hostname.

```
NetWare 3.11 License Validation Key
abcde12345
```

The License Validation Key is on the key sheet that ships with the Services license. The key is a ten–character alphanumeric code; it is case–sensitive, so type it exactly as it appears on the license key sheet. We use **abcde12345** in our example.

NOTE: If you have a five–user license, accept the default at the License Validation Key prompt.

Answer **Y** to the server failover prompts.

```
Install this NetWare server with Failover
support? [N] Y
Is this host the PRIMARY Failover server?
[Y]? Y
```

Enter the TCP/IP name of your secondary host; it should be defined in your **/etc/hosts** file. We use the hostname **development** in our example.

```
Hostname of SECONDARY host? development
```

NetWare setup scripts then display additional prompts and perform the tasks necessary to set up your primary server for a machine–initiated failover.

The system displays status messages along with the prompts, as indicated below.

```
File Server Name production
NetWare 3.11 License Validation Key abcde12345
Install this NetWare server with Failover
support? [N] Y
Is this host the Primary Failover server? [Y] Y
Primary NetWare Failover system.
Setting up NetWare Services for Failover...
This script needs to know the hostname of the
SECONDARY host in the NetWare failover
configuration
Hostname of SECONDARY host? development
```

3. Answer the following prompt.

```
Virtual disks to be 'failed
over'[usr_opt_netware usr_netware]
```

When answering this prompt:

- Specify the NetWare–related virtual disks you want to be switched over from the primary host to the secondary host if a system failure occurs. Typically, the defaults are **usr_opt_netware** and **usr_netware**.
- Specify **usr_opt_netware** and **usr_netware** and include any additional virtual disks that will be defined as NetWare volumes.

The system displays the status message:
`Checking virtual disk`
while searching for each virtual disk that you entered or confirmed. If the system finds the virtual disk, it adds `OK` to the status message. Otherwise, it adds
`Does not exist.` to the status message.

The system displays status messages similar to the following.

```
This script needs to know the names of the
virtual disks that should be 'failed over' from
the PRIMARY host to the SECONDARY host in the
event of primary host failure.

Virtual disks to be 'failed over'
   [usr_opt_netware usr_netware]
Checking virtual disk usr_netware...OK
Checking virtual disk usr_opt_netware...OK
```

Then the system displays a list of virtual disks that it has confirmed to exist, similar to the one below.

```
List of virtual disks to be 'failed over':
usr_netware  usr_opt_netware
```

4. Answer the following prompt.

```
Is this list OK [no] ? Y
```

Verify that the listed virtual disks are the ones you want to switch over to the secondary server if a system failure occurs. If the list is correct, answer **Y**. Otherwise, answer **N**, and the system prompts you again for the names of the virtual disks you want to switch over.

5. Answer the following **sysadm** prompt.

```
Physical disks to be 'failed over'
   sd(ncsc (0,6),2,0)
```

The physical disks listed after this prompt are the virtual disks you previously selected.
List the names of any other the physical disks that you want to switch over if a system failure occurs. Usually, you can accept the default (as we do in our example).

CAUTION: File systems on the physical disks you list will be mounted when the secondary server takes over the disks after a system failure. Therefore, the physical disks you list should not contain any parts of virtual disks that are not being switched over. If they do, these physical disks may not correctly switch over to the secondary server.

If you are not sure if the physical disks you want to use to meet the above restriction, you should stop the setup, change your virtual disk layouts, and then restart the installation with server failover.

The system displays status messages along with the prompt, as indicated below.

```
This script needs to know the names of the
physical disks that should be 'failed over' from
the PRIMARY host to the SECONDARY host in the
event of primary host failure.
Physical disks to be 'failed over'
   sd(ncsc (0,6),2,0)
```

6. Answer the following **sysadm** prompt.

```
Is this list OK [No] ? Y
```

If the list of physical disks is correct, answer **Y**. Otherwise, answer **N**, and the system prompts you again for names of the physical disks you want to switch over to the secondary server if a system failure occurs.

7. Answer the following **sysadm** prompt by entering a secondary host physical disk specification for each primary host physical disk specification. We use **sd(ncsc (0,7),2,0)** in our example.

```
SECONDARY system disk specification:
    sd(ncsc (0,7),2,0)
```

Do not enter a secondary host physical disk specification that is identical to the corresponding primary host physical disk specification. It is illegal for two computers to use the same SCSI value for a shared drive.

CAUTION: If you fail to enter a valid secondary host physical disk specification for a primary specification, the system will not correctly switch that physical disk over to the secondary server after a system failure.

The system displays status messages along with the prompt, as indicated below.

```
For each physical disk on the PRIMARY system that
can be 'failed over', this script needs to know
the specification of the physical disk on the
SECONDARY system. You will be prompted now to
supply this information.

PRIMARY system disk specification:
   sd(ncsc (0,6),2,0)
SECONDARY system disk specification:
   sd(ncsc (0,7),2,0)

Physical disks:
   PRIMARY              SECONDARY
  ----------            ----------
sd(ncsc (0,6),2,0)     sd(ncsc (0,7),2,0)
```

8. Answer the following prompt.

```
Is this table OK [no] ? Y
```

If the specification(s) for the secondary physical disk(s) are correct, answer **Y**. Otherwise, answer **N**, and the system prompts you again for the specification(s).

Then the system displays messages indicating that the Service package has successfully loaded.

```
   Setting up failover disk on PRIMARY system ...
Physical disk (sd(ncsc (0,6),2,0) has been added.
   Setting up failover disk database on SECONDARY
   system ...
Synchronization complete for host development
   Setting up monitor database on SECONDARY
   system.
Failover monitors file entry for production has
been added.
Failover monitor for production has been started.
   NetWare Failover Setup Complete...
```

```
Package nw_serv has been successfully set up in
MY_HOST root.
Package setup for nw_serv is complete.
```

9. If you are installing Services on an existing system, run **nwrestore**. See the section "Restoring the file attributes and trustee rights" in Chapter 2 for instructions on running **nwrestore**.

Continue the installation with the next section.

Rebooting the primary server

Follow these steps.

1. Exit **sysadm**.

1. Move to the root directory. Type:

   cd / ↵

2. Type:

   shutdown -g0 -y ↵

   halt -q ↵

3. Reboot the system and return to init level 3.

NOTE: If you are upgrading from Revision 2.xx, the first time you start NetWare, the system takes longer than usual to reboot as it must rebuild the inodes files.

Continue the installation with the next section.

Installing Transport software with failover on the secondary server

Follow these steps.

IMPORTANT: Because DG/UX failover does not allow a server to have more than one virtual disk with the same name, your secondary server cannot have **usr_opt_netware** and **usr_netware** virtual disks. If you plan to set up server failover using an existing NetWare server as a secondary server, you should remove **usr_opt_netware** and **usr_netware** virtual disks, and any other virtual disks that are typically named on the primary server.
If virtual disks with the same name exist on the primary and secondary servers when you install Transport software with server failover, the system prompts you to delete these virtual disks.

1. If you are installing Transport software with server failover on a new system, follow *all but the last step* in the section "Installing the Transport software" in Chapter 2.

   If you are installing Transport software with server failover on an existing system, follow *all but the last step* in the section "Installing Transport over existing software" in Chapter 2.

   Then continue the server failover setup with the next step.

2. Answer the following **sysadm** prompts.

   ```
   System Name?: [development] development

   Install this NetWare server with Failover
   support? [N] Y
   ```

```
Is this host the PRIMARY host? [Y] N
```

The system displays status messages along with the prompts, as indicated below.

```
The NetWare transport needs to add items to the
system build files in order to complete the
installation.  This step will verify that these
items are properly added before attempting to build
the system.
System Name?: [development] development
Install this NetWare server with Failover support?
 [N]? Y
Is this host the PRIMARY Failover server? [Y]? N
SECONDARY NetWare Failover system
*** WARNING ***
NetWare setup must delete /usr/opt/netware and
/usr/netware on the secondary host as part of
the setup.
```

3. Answer the following **sysadm** prompt.

```
Continue with failover setup? [N] Y
```

If you plan to use an existing NetWare server as a secondary server when setting up server failover, you should remove the **usr_opt_netware** and **usr_netware** virtual disks, and any other virtual disks that have the same VDU (virtual disk unit) name on the primary server.

NOTE: The system will not delete the parts of these virtual disks that it needs to complete the installation. Therefore, you must run **nw_failover_cleanup_secondary** (as explained in the next section) after you finish installing Transport with server failover on the secondary server.

If you have deleted the appropriate virtual disks, answer **Y**. Otherwise, answer **N**, to stop the Transport installation process. Then, on the primary and secondary servers, delete the virtual disks with identical names. Then restart the Transport installation process.

The system displays status messages along with the prompts, as indicated below.

```
   Continue with failover setup? [N] Y
   Setting up NetWare Transport for Failover ...
   NetWare Failover Setup Complete...
Configuring system...
Building kernel...
Successfully built dgux.development.
Linked /dgux. You must reboot in order for this kernel
to take effect.
   *** NOTE ***
   You must run
/etc/failover/nw_failover_cleanup_secondary
after the package load is complete. This script
completes the cleanup of NetWare on your secondary
failover system.
Installation of NetWare 3.11/Transport is complete.
Package nw_tran has been successfully set up in MY_HOST
root.
Package setup for nw_tran is complete.
```

Continue the installation with the next section.

Running nw_failover_cleanup_secondary

Finish setting up the secondary server by running the **nw_failover_cleanup_secondary** utility. Running this utility deletes all or any parts of the (default) virtual disks **usr_opt_netware** and **usr_netware**, that might remain on the secondary server. You run this utility on the secondary server only.

CAUTION: *If you fail to run **nw_failover_cleanup_secondary** to remove all or any remaining parts of **usr_opt_netware** and **usr_netware** virtual disks after installing Transport on the secondary server, the system will not switch these virtual disks over to the secondary server if a system failure occurs.*

Follow these steps.

1. Optionally, back up the **usr_opt_netware** and **usr_netware** virtual disks if you intend to access or restore them in the future. See *Managing the DG/UX™ System* for instructions on backing up these virtual disks.

NOTE: You can use **usr_opt_netware** and **usr_netware** virtual disks only on a NetWare system set up *without* server failover.

2. Move to the appropriate directory. Type:

   cd /etc/failover ↵

3. Run the cleanup utility. Type:

   ./nw_failover_cleanup_secondary ↵

4. Answer this prompt.

   ```
   Is the local host the SECONDARY host? [N] Y
   ```

5. Answer this prompt.

```
Virtual disks to be erased and removed:
[usr_opt_netware  usr_netware]
```

Type the names of virtual disks you want removed from the secondary server. Or you can accept the default. (We accept the default in our example.)

The system displays the status message:
`Checking virtual disk xxx_yyy_zzz`
while searching for each virtual disk that you entered or confirmed. If the system finds the virtual disk, it adds `OK` to the status message. Otherwise, it adds `Does not exist.` to the status message.

The system displays status messages similar to the following.

```
Virtual disks to be erased or removed?
   [usr_opt_netware usr_netware]
Checking virtual disk usr_netware...OK
Checking virtual disk usr_opt_netware...OK

List of virtual disks to be erased or removed:
usr_opt_netware usr_netware
```

6. Answer the following prompt.

```
Is this list OK [no] ? Y
```

If the list of virtual disks is correct, answer **Y**. Otherwise, answer **N**, and the system prompts you again for a list of virtual disks to be removed or erased.

When the system is finished, it displays:

```
Done.
```

Continue the installation with the next section.

Rebooting the secondary server

Follow these steps.

1. Exit **sysadm**.

1. Move to the root directory. Type:

   cd / ↵

2. Type:

   shutdown -g0 -y ↵

   halt -q ↵

3. Reboot the system and return to init level 3.

NOTE: If you are upgrading from Revision 2.xx, the first time you start NetWare, the system takes longer than usual to reboot as it must rebuild the inodes files.

Procedures for installing the Transport and Services software and setting up server failover on the primary and secondary server are now finished. If you want to ensure that your printers work after a system failover on a NetWare system, follow procedures in the section "Setting up NetWare to continue printing after failover."

The next section describes scripts you can use to modify server failover procedures after you finish the NetWare installation.

Modifying server failover with scripts

This section lists and describes scripts that you can use to change the default settings of the server failover process. These scripts were installed when you installed NetWare software with server failover.

NetWare usually locates these scripts in **/etc/failover**. However, if failover was already set up for other disks or applications, NetWare locates these scripts in **/usr/opt/netware/failover**.

This table gives the name and purpose of scripts that NetWare creates and uses for DG/UX failover.

Script name	Purpose
NW_lost_pulse	• Invoked by the failover monitor when the secondary host can no longer contact the primary host over the defined communication paths. • Used only on secondary (backup) host
NW_regained_pulse	• Invoked by the failover monitor when the primary host has returned • Used only on the secondary (backup) host. Currently does not take any action to return NetWare for AViiON to the primary system upon its return. The system administrator can decide when to manually switch the disks back to the primary system.
stop_NW_failover	• Available on the secondary host • Used to stop NetWare for AViiON and, if necessary, NetWare Services in preparation for returning the disks to the primary server
give_NW_to_primary	• Available on the secondary host • Contains commands required to return NetWare disks to the primary host • Should be run after NetWare has been stopped through stop_NW_failover
NW_virtualdisks	• Lists virtual disks containing the NetWare product and physical disks containing NetWare volumes. NetWare uses this listing to properly set up the failover relationship between the primary NetWare system and its backup.
start_NW_failover	• A failover application script that the failover software automatically runs when the disks containing NetWare are moved to the backup system. • Also automatically runs when the disks are switched back to the primary system.

Setting up NetWare to continue printing after failover

This section gives procedures to ensure that you can continue NetWare printing after a system failure occurs on a NetWare system installed with server failover.

Follow these steps.

1. Create the same DG/UX print queue names on the primary and secondary systems. Identical DG/UX print queue names must exist on both the primary and secondary servers for printers defined to NetWare through SCONSOLE. Otherwise, NetWare errors and possible loss of print requests can occur after a server failover.

2. Do one of the following.

   - Have the queues you created in step 1 associated with physical printers attached to both servers.

     If the printers are connected directly to the AViiON systems, this would require additional printer hardware.

   - Have the queues you created in step 1 associated with DG/UX remote printers that reside on the primary server.

     When the primary server comes back on line, the print requests will process.

   - Have the queues you created in step 1 associated with LAN–based printers.

     This action reduces the need for additional printers, as primary and secondary servers can share printers on the LAN.

Where to go from here

Use this information to determine where to continue the NetWare network installation process.

If you need to	See
Install a DOS Workstation	*NetWare Requester for DOS*
Install an OS/2 workstation	*NetWare Requester for OS/2*
Install a MacIntosh workstation	*NetWare for MacIntosh Installation and Maintenance*
Install a router (bridge)	Chapter 3 – "Router Installation Management"
Install cabling	Installation supplements or documentation that ships with your network boards
Set up diskless workstations	*NetWare Requester for DOS*
Create users, directories, and network security	Chapter 4 – "Network File Services Setup"

End of Appendix

Index

A

Account balance, 4-66
  See also Accounting

Account management, 4-66
  See also User Account Manager; Workgroup Manager

Account restrictions
  assigning system defaults, 4-66
  assigning to users, 4-77
  planning for a user, 4-25
  planning system defaults, 4-19
  See also Disk space; Login restrictions

Accounting
  assigning an account balance to a user, 4-78
  assigning system defaults, 4-66
  installing, 4-65
  planning for a user, 4-25
  planning system defaults, 4-18

After installing NetWare on Trusted DG/UX, C-12

After installing or upgrading NetWare, 2-32

Application directories
  loading application files into, 4-58
  loading data files into, 4-64
  planning directory structure, 4-6
  search drives in login scripts, 4-47
  security, 4-35, 4-41

Applications
  and AUTOEXEC.BAT file, 4-64
  and CONFIG.SYS file, 4-64
  copy protection, 4-41, 4-60
  installing on the network, 4-58
  planning directories for, 4-6
  setting file attributes with FLAG, 4-59

ATTACH, in login script, A-9

Attributes security, 4-38
  assigning for application program files, 4-59
  assigning for DOS files, 4-57
  defaults for files in system–created directories, 4-34
  planning, 4-34

B

Backing up files and trustees rights, 2-15

Batch file directories
  planning directory structure, 4-7
  planning security, 4-42
  security, 4-37

Boot disk, router
  copying the ROUTER.EXE file to, 3-5
  creating on diskette, 3-5
  creating on hard disk, 3-5
  creating the AUTOEXEC.BAT file on, 3-6

Boot disk, workstation
modifying AUTOEXEC.BAT, 4-64
modifying CONFIG.SYS, 4-64

BREAK in login script, A-12

C

Charge rates, 4-18, 4-21

Comments in login scripts, 4-45, A-49

Common directories, planning, 4-7

Compound strings in login scripts, A-54

COMSPEC, in login scripts, 4-46, A-13

CONFIG.SYS, modifying on boot disk, 4-64

Configuring network printers with pconfig, 2-28–2-31

Connections, restricting concurrent, 4-20, 4-31, 4-78

Console operator, viewing user's status, 4-81

Contacting Data General, xi

Copy protection for applications, 4-41, 4-60

Copying LAN drivers to diskette, 3-2

Copying ROUTGEN to diskette, 3-1

Creating hybrid users, 4-94

Credit limits, 4-22

D

Data files, loading into directories, 4-64

Data General, contacting, xi

Database directories
backup, simplifying, 4-6, 4-7
planning attribute security for directories and files, 4-41
rights, 4-36

Delete Inhibit attribute, assigned, 4-59

Deleting virtual disks, when installing server failover, D-19, D-22

Directories
creating, 4-57
displaying path, 4-41
DOS, creating, 4-6, 4-56
DOS, planning, 4-6
home (username), 4-21, 4-76, 4-82
shareable, 4-7
system–created, 4-5

Directory security
assigning trustees, 4-70
attributes, 4-40
Inherited Rights Mask, 4-33
planning attributes, 4-38

Directory structure
creating, 4-57
example, 4-8
host, 4-3
hybrid, 4-3
planning, 4-3

Disk space, planning restrictions, 4-30

DISPLAY, in login script, A-15

Document sets, v

DOS BREAK, in login script, A-17
DOS directories
  accessing through system login script, 4-46
  creating, 4-56
  naming conventions, 4-56
  planning, 4-6
  planning security for, 4-35
  setting file attributes for, 4-56
DOS files, security planning, 4-40
DOS, installing on the network, 4-55
DOS SET, in login script, A-18
DOS VERIFY, in login script, A-21
DRIVE, in login script, A-22
Drive mappings
  fake root, 4-58
  in system login script, 4-43, 4-46
  to application directories, 4-47
  to DOS directories, 4-46
  to home (username) directories, 4-47
  to NetWare utilities, 4-46

E

Editing server failover scripts, D-25
Environmental requirements, 1-2
ERROR_LEVEL identifier variable, A-30
EVERYONE (group)
  planning security for, 4-34
  system–created, 4-10
EXIT, login script, 4-49, 4-51, A-23
External program execution from login script, 4-49

F

Fake root, mapping, 4-58, A-43
FDISPLAY, in login script, A-25
File attributes, 4-59
  See also attributes security
File server
  attaching to additional, 4-46
  services, charging for, 4-18
  See also Accounting
FILER utility
  accessing, 4-60
  creating directories, 4-54
  creating DOS directories, 4-55
  viewing a file's Inherited Rights Mask, 4-61
Files
  loading DOS, 4-57
  setting attributes, 4-59
FIRE PHASERS, in login script, A-27
FLAG utility, setting file attributes, 4-57, 4-59

G

GOTO, in login script, A-28
Groups
  adding users to, 4-85
  and Workgroup Manager, 4-69, 4-80
  assigning trustee file rights to, 4-72, 4-82
  creating, 4-69, 4-85
  creating trustee assignments in, 4-84
  EVERYONE (system–created), 4-10
  planning, 4-13, 4-28
  planning trustee assignments in, 4-36, 4-37
  workspace, 4-36

GUEST (user)
directory, planning security for, 4-36
security in an application, 4-36
system–created, 4-10

H

Hard disk, local, mapping as network drive, 4-58

High availability methods, D-2
multi–path LAN I/O, D-2
server failover, D-2

Host directory structure, 4-3

How multi–path LAN I/O works, D-2

How server failover works, D-2, D-4–D-5

Hybrid directory structure, 4-3

Hybrid NetWare users on Trusted DG/UX, required hybrid status, C-10

Hybrid users
create, 4-94
planning, 4-11, 4-34

I

Identifier variables
listed, A-30
MACHINE, A-41
MEMBER OF, A-31
NETWORK_ADDRESS, A-31
OS, A-41
OS_VERSION, A-41
P_STATION, A-32
SMACHINE, A-41

Identifier variables in login script(s), A-29, A-54
ERROR_LEVEL, A-30
listed, A-4
used with different DOS versions, A-55

IF...THEN...ELSE, in login script, A-29

INCLUDE, in login script, A-37

Inherited Rights Mask, viewing for a file, 4-61

Initial hardware setup, 1-3

Installation roadmap, 1-3

Installation tasks
new installation on Trusted DG/UX, C-2
upgrading from R. 1.xx, 2-14

Installing NetWare, existing systems
backing up existing files and trustees rights, 2-15
installing Services software, 2-20–2-24
installing Transport software, 2-17–2-24

Installing and generating router software, 3-2–3-4

Installing NetWare, creating virtual disks and file systems, 2-3–2-6

Installing NetWare on a new system
installing the software, 2-6–2-12
installing Services software, 2-10–2-16
installing Transport software, 2-7–2-10
rebooting the server, 2-13–2-16
tasks, 2-2
rebooting the server, 2-25
tasks, 2-14
upgrading from R. 1.xx, 2-14
Installing NetWare on Trusted DG/UX
creating virtual disks and file systems, C-3
finishing the installation, C-10–C-12
installing Services software, C-9
installing Transport, C-4–C-9
rebooting the server, C-9
Installing NetWare with server failover, D-6–D-24
deleting virtual disks, D-19, D-22
installing Services on the primary server, D-11–D-28
installing Transport on the primary server, D-8–D-28
installing Transport on the secondary server, D-19–D-28
nw_failover_cleanup_secondary, D-22
preparing to install, D-7
rebooting the primary server, D-18
rebooting the secondary server, D-24
specifying physical disks, D-15–D-18
specifying virtual disks, D-13
tasks, D-6
Intruder Detection/Lockout
planning, 4-23, 4-28
setting, 4-80

L

Local hard disk, mapping as network drive, 4-58

LOGIN directory, 4-3

Login restrictions
intruder lockout, 4-24, 4-80
limiting concurrent connections, 4-20, 4-31, 4-67
locking a user account, 4-24, 4-80
password(s), 4-21, 4-27, 4-77, 4-78
station restrictions, 4-20, 4-29, 4-66, 4-77
time restrictions, 4-22, 4-29, 4-66, 4-77
tracking logins, 4-18

Login restrictions, 4-66
See also Account Restrictions, passwords

Login script
compound strings in, A-54
conditionals, A-34
conventions, 4-44, A-6
creating, 4-90
examples, A-56
explained, 4-43, A-1
mapping drives, 4-46, A-40
security, A-1
planning, 4-44
See also Login script, user

Login script commands
ATTACH, A-9
BREAK, A-12
COMSPEC, A-13
DISPLAY, A-15
DOS BREAK, A-17
DOS SET, A-18
DOS VERIFY, A-21
DRIVE, A-22
EXIT, A-23
FDISPLAY, A-25
FIRE PHASERS, A-27
GOTO, A-28
IF...THEN...ELSE, A-29
INCLUDE, A-37
listed, A-4
MACHINE, A-39
MAP, A-40
PAUSE, A-47
PCCOMPATIBLE, A-48
PCCOMPATIBLE , A-48
REMARK, A-49
SHIFT, A-51
WRITE, A-54

Login script, user
copying from one user to another, 4-93
creating, 4-90, 4-92
examples, 4-51, A-59
mapping drives, 4-51, A-40
modifying, 4-93
planning, 4-51
stored in SYS:MAIL, 4-5

LOGIN utility, exiting from login script, A-24

Long machine name, in DOS directories, 4-56

M

MACHINE identifier variable, A-41

MACHINE, in login script, A-39

MAKEUSER, planning to create users with, 4-14

Managing routers, 3-5–3-7

MAP ROOT, in login script, A-43

MAP utility, mapping drives in login script, A-40

Mapping, A-1
See also Drive mapping

MEMBER OF identifier variable, A-31

Menu, executing from user's login script, 4-51

Modifying server failover scripts, D-25
creating, 4-92
modifying, 4-93

Multi–path LAN I/O, how it works, D-2

N

NCOPY utility, copying files with, 4-57

NDAY in login scripts, A-4

NetWare auditable events, system masks, C-11

NetWare users on Trusted DG/UX, required hybrid status, C-10

NetWare with server failover
after a system failover, D-5
before a system failover, D-4

Network drives, mapping in login scripts, 4-43, A-40

Network environment, planning, 4-1

NETWORK_ADDRESS identifier variable, A-31

New Line key, viii

Notational conventions in this manual, viii

nwbackup, backing up existing files and trustees rights, 2-15, 2-21

nwrestore, restoring files and trustees rights, 2-26

O

OS identifier variable, A-41

OS_VERSION identifier variable, A-41

P

P_STATION identifier variable, A-32

Password
- assigning, 4-78
- planning, 4-21
- setting system defaults for, 4-66

PAUSE, in login script, A-47

PCCOMPATIBLE, in login script, A-48

pconfig procedures for configuring DG/UX printers, 2-28–2-31

pconfig restrictions, 2-28

Power surge protection, 1-2

Print job configurations stored in SYS:MAIL, 4-5

Printer mappings, in login scripts, 4-48

Printing after a system failover, setup with server failover, D-27

PROMPT, display directory path, 4-56

Prompt, display directory path, 4-49

PUBLIC directory, 4-3
See also SYS:PUBLIC

Public files in SYS:PUBLIC, 4-5

R

Rates, charge, 4-21

Rebooting
- primary server with failover, D-18
- secondary server with failover, D-24
- server, when installing a new or existing system, 2-13, 2-25

Related manuals, v

REMARK, in login script, 4-45, A-49

Restoring files and trustees rights, 2-26

Rights
- assigning, 4-82
- assigning trustees, 4-70, 4-72
- in root directory, A-43
- list of, 4-34
- planning, 4-32

Root directory, users' rights, A-43

Root, fake, 4-58, A-43

ROUTEGEN utility, 3-2–3-4

Router
creating a boot diskette, 3-5
installing, 3-2
setup, 3-5

ROUTER.EXE, copying to router boot disk, 3-5

Running failover_cleanup_secondary, D-22

S

Search drive mappings
application directories, 4-47
creating in login scripts, A-42
DOS directories, 4-46
NetWare utilities, 4-46
system login scripts, 4-46

Security
equivalence, 4-29, 4-81
login scripts, A-1
passwords, 4-21
See also Password
recommendations for directories and files, 4-34
rights, 4-21
See also Rights

Server failover
how it works, D-2, D-4–D-5
script names and description, D-26
scripts, D-6, D-7, D-25–D-26
setting up printers to continue after failover, D-27

Server failover installation
deleting virtual disks, D-19, D-22
installing Services on the primary server, D-11–D-28
installing Transport on the primary server, D-8–D-28
installing Transport on the secondary server, D-19–D-28
preparing to install, D-7
rebooting the primary server, D-18
rebooting the secondary server, D-24
running failover_cleanup_secondary, D-22
specifying physical disks, D-15–D-18
specifying virtual disks, D-13
tasks, D-6

Shareable directories, planning, 4-7

SHIFT, in login script, A-33, A-51

SMACHINE identifier variable, A-41

Specifying physical disks, when installing server failover, D-15–D-18

Specifying virtual disks, when installing server failover, D-13

Station restrictions, assigning, 4-77

SUPERVISOR (user)
account, accessing, 4-25
password, 4-56

Supervisor responsibilities, 4-10, 4-12
See also User Account Manager, Workgroup manager

SYS:LOGIN, explained, 4-5

SYS:MAIL, 4-5
login scripts stored in, 4-43
rights of EVERYONE in, 4-43

SYS:PUBLIC, 4-5

SYS:SYSTEM, 4-5
SYSCON
  creating groups, 4-69
  creating users, 4-74
  setting system default restrictions, 4-66
  trustee rights, 4-70, 4-72
SYSCON utility
  accounting, 4-65
  assigning User Account Managers, 4-89
  assigning Workgroup Managers, 4-87
  creating groups, 4-79, 4-85
  creating system login script, 4-90
  creating users' login scripts, 4-92
  home (username) directories, 4-82
  passwords, 4-79
  restrictions to users, 4-77
  system login script, 4-90
  time and login restrictions, 4-77
  trustee assignments, 4-82
  User Account Managers, 4-81
  users' login scripts, 4-92
  Workgroup Managers, 4-80

T

Time restrictions, assigning, 4-66, 4-77, 4-81
  See also Login restrictions

Transport configuration settings, 2-12

Trustee assignments
  assigning, 4-82
  creating, 4-70, 4-72
  explained, 4-33
  See also Rights

U

User Account Manager
  creating, 4-80, 4-81, 4-89
  planning, 4-28
  responsibilities, 4-12

User Account Manager
  See also Workgroup Manager

User accounts
  assigning, 4-80
  creating system defaults, 4-66
  planning for a user, 4-25
  planning system defaults, 4-19
  viewing ID number, 4-81

User ID number, viewing, 4-81

USERDEF, planning to create users with, 4-14

Username directory, 4-6
  creating, 4-54, 4-76, 4-82
  making trustee assignments to, 4-82
  mapping drives to, 4-48
  planning, 4-6, 4-21
  security, 4-36

Usernames, planning, 4-11

Users
  adding to groups, 4-85
  GUEST, system–created user, 4-10, 4-36
  planning, 4-10, 4-16
  restrictions, 4-77
  See also Accounting restrictions; Disk space; Login restrictions
  station restrictions, 4-81
  SUPERVISOR, system–created user, 4-10
  time restrictions, 4-81
  trustee directory rights, 4-82
  trustee file rights, 4-82

Users, 4-74, 4-77
  See also User accounts

V

Variables (identifier), in login script, A-4

W

Workgroup Manager
creating, , 4-28, 4-69, 4-75, 4-80, 4-87
planning, 4-12
responsibilities, 4-12
See also User Account Manager

Workgroups
creating, 4-69
managing, 4-12
planning, 4-12, 4-28
See also Groups

WRITE in login script, A-54

NetWare® for AViiON® Systems: Installation

069–000488–06

Cut here and insert in binder spine pocket