Supermax LAN Manager/X

System Administrator's Guide

July, 1991
Version 1.0

Stock No. 94423221

© 1991
Dansk Data Elektronik A/S

CONTENTS

1. Introduction 1-1
1.1. Overview 1-1
1.2. What's in This Guide? 1-1
1.3. Prerequisites for Administering LAN Manager 1-2
1.4. Conventions Used in This Guide 1-3

2. Understanding the Server Program 2-1
2.1. Overview 2-1
2.2. Server Program Features and Services 2-1
2.2.1. File and Print Services 2-1
2.2.2. Remote Administration 2-1
2.2.3. Shared Client Printers 2-1
2.2.4. Network Message Service 2-2
2.2.5. Audit Trail 2-2
2.2.6. Text File Translation 2-3
2.2.7. DDE-Term Terminal Emulation 2-3
2.2.8. Remote UNIX System Process Execution 2-3
2.3. LAN Manager Resource Security 2-4
2.3.1. Logon Validation and Scripts 2-4
2.4. The Administrator's Role 2-5

3. Using the Administrative Interfaces 3-1
3.1. Overview 3-1
3.2. The Administrative Interfaces 3-1
3.3. Using the Full Screen Net Admin Interface 3-2
3.3.1. Accessing the Full Screen Net Admin Interface 3-2
3.3.2. Working With the Full Screen Net Admin Interface 3-3
3.3.2.1. Understanding the Screen Display for the Full Screen Net Admin Interface 3-4
3.3.2.2. Using the Dialog Boxes 3-7
3.3.2.3. Moving Around in a Dialog Box 3-8
3.3.2.4. Using Text Boxes 3-9
3.3.2.5. Using List Boxes 3-10
3.3.2.6. Using Check Boxes 3-14
3.3.2.7. Using Option Buttons 3-14
3.3.2.8. Using Command Buttons 3-15
3.3.2.9. Using Display Fields 3-16
3.3.3. Exiting the Full Screen Net Admin Interface 3-16
3.4. Administering the Server from the UNIX System 3-17
3.4.1. Using the Default UNIX System Administrative User Login 3-17

4. Setting Up a User-Level Security Server 4-1
4.1. Overview 4-1
4.2. What Is User-Level Security? 4-1
4.2.1. Understanding User Accounts 4-2

4.2.2. Understanding User Groups 4-2
4.2.3. Understanding Privileges 4-3
4.2.4. Understanding Access Permissions 4-3
4.2.4.1. Disk Resource Access Permissions 4-4
4.2.4.2. Shared Print Queue Access Permissions 4-6
4.2.5. How LAN Manager Determines Access to Resources 4-6
4.2.5.1. Summary of Access Permissions 4-7
4.3. Planning the Server Configuration 4-8
4.3.1. Determining Users and Groups 4-8
4.3.2. Determining Shared Resources 4-9
4.3.2.1. Default Shared Directories 4-10
4.3.2.2. Organizing Server Files and Directories 4-11
4.3.2.3. Recommended Locations for Creating New Shared Directories 4-11
4.3.3. Determining Access to Resources 4-13
4.4. Implementing the Server Configuration 4-14
4.4.1. Starting the Client Program 4-15
4.4.2. Logging On as the Administrator 4-15
4.4.3. Setting Up Logon Validation 4-16
4.4.4. Setting Up the Alerter Service 4-18
4.4.5. Setting Up Resource Auditing (Audit Trail) 4-19
4.4.6. Creating New User Groups 4-20
4.4.6.1. Equivalent net Command 4-22
4.4.7. Creating New User Accounts 4-22
4.4.7.1. Equivalent net Command 4-28
4.4.8. Sharing Directories 4-28
4.4.8.1. Equivalent net Command 4-32
4.4.9. Setting Up Shared Print Queues 4-32
4.4.9.1. Configuring Printers 4-32
4.4.9.2. Sharing Print Queues 4-33
4.4.9.3. Equivalent net Command 4-38

5. Managing Server Operations 5-1
5.1. Overview 5-1
5.2. Stopping and Restarting the Server 5-1
5.2.1. Stopping the Server Program 5-1
5.2.2. Restarting the Server Program 5-2
5.3. Displaying the Audit Trail 5-2
5.4. Listing Servers and Resources Available on the LAN 5-4
5.4.1. Listing Visible Servers 5-4
5.4.2. Listing Shared Server Resources 5-4
5.4.3. Equivalent net Command 5-7
5.5. Clearing or Changing an Administrative Password 5-7
5.5.1. Equivalent net Command 5-8
5.6. Running the Command-Line Administration Utility 5-8

6. Managing Users and Groups Under User-Level Security 6-1
6.1. Overview 6-1

6.2. Managing Users 6-1
6.2.1. Adding User Accounts 6-2
6.2.1.1. Equivalent net Command 6-10
6.2.2. Changing User Passwords 6-10
6.2.2.1. Equivalent net Command 6-11
6.2.3. Removing User Accounts 6-11
6.2.3.1. Equivalent net Command 6-12
6.2.4. Displaying Existing User Accounts 6-12
6.3. Managing Groups 6-13
6.3.1. Adding New Groups Using the Full Screen Net Admin Interface 6-13
6.3.1.1. Equivalent net Command 6-15
6.3.2. Adding Members to an Existing Group 6-15
6.3.2.1. Equivalent net Command 6-16
6.3.3. Managing the uexec Group 6-17
6.3.4. Removing Members from a Group 6-18
6.3.4.1. Equivalent net Command 6-18
6.3.5. Removing Groups 6-19
6.3.5.1. Equivalent net Command 6-19

7. Managing Shared Directories 7-1
7.1. Overview 7-1
7.2. Listing Shared Directories 7-1
7.2.1. Listing Shared Directories by Using the Full Screen Net Admin Interface 7-1
7.2.2. Listing Shared Directories by Using the Command Line Net Interface 7-2
7.3. Sharing Directories 7-2
7.3.1. Equivalent net Command 7-8
7.4. Managing Disk Resource Access Permissions 7-8
7.4.1. Understanding Disk Resource Access Permissions 7-8
7.4.2. Looking at Access Permissions 7-10
7.4.3. Changing Access Permissions for Disk Resources 7-11
7.4.4. Equivalent net Command 7-14
7.4.5. Changing Access Permissions as a Non-Administrative User 7-14
7.4.6. Assigning Default and Inherited Access Permissions 7-14
7.4.7. Equivalent net Command 7-17
7.5. Unsharing Directories 7-17
7.5.1. Equivalent net Command 7-18
7.6. Maintaining a Shared Disk 7-18
7.6.1. Managing Server Disk Space 7-19
7.6.2. Backing Up and Restoring Server Files 7-20

8. Managing Shared Printers 8-1
8.1. Overview 8-1
8.2. Understanding Shared Print Queues 8-1
8.2.1. How Do Shared Print Queues Work? 8-2

8.2.2. Options for Shared Print Queues 8-2
8.2.2.1. The Printer Devicename Option 8-3
8.2.2.2. The Queue Priority Option 8-4
8.2.2.3. The Scheduling Option 8-4
8.2.2.4. The Print Processor Option 8-4
8.2.2.5. The Parameters Option 8-5
8.2.2.6. The Separator Page Option 8-5
8.3. Creating Shared Print Queues 8-5
8.3.1. Creating a Shared Print Queue by Using the Full Screen Net Admin Interface 8-5
8.3.1.1. Equivalent net Command 8-11
8.3.2. Assigning Access Permissions for Printer Resources 8-11
8.3.3. Defining Customized Print Processor Scripts 8-13
8.3.3.1. Guidelines to Use When Defining Scripts 8-13
8.3.3.2. Environmental Variables that Can Be Included in Scripts 8-14
8.3.3.3. Sample Scripts 8-14
8.3.3.4. Defining Scripts by Using a Text Editor 8-14
8.3.4. Making Shared Print Queues Unavailable 8-15
8.3.4.1. Unsharing Shared Print Queues by Using the Full Screen Net Admin Interface 8-15
8.3.4.2. Equivalent net Command 8-16
8.4. Managing Shared Print Queues and Print Jobs 8-16
8.4.1. Changing Shared Print Queue Options 8-16
8.4.1.1. Equivalent net Command 8-19
8.4.2. Changing Shared Print Queue Status 8-19
8.4.2.1. Equivalent net Command 8-21
8.4.3. Controlling Printers by Sharename 8-21
8.4.3.1. Equivalent net Command 8-23
8.4.4. Listing and Controlling Print Jobs 8-23
8.4.4.1. Equivalent net Command 8-26

9. Changing the Default Server Configuration 9-1
9.1. Overview 9-1
9.2. Understanding How the Server Is Configured 9-1
9.3. Understanding the lanman.ini File 9-1
9.3.1. The Syntax of the lanman.ini File 9-2
9.3.2. The Organization of the lanman.ini File 9-3
9.3.3. The *[server]* Section of the lanman.ini File 9-4
9.3.4. The [lmxserver] Section of the *lanman.ini* File 9-8
9.3.5. The [workstation] Section of the *lanman.ini* File 9-29
9.3.6. The [netlogon] Section of the *lanman.ini* File 9-29
9.3.7. The [uidrules] Section of the *lanman.ini* File 9-29
9.3.8. The [ups] Section of the *lanman.ini* File 9-30
9.3.9. A Sample *lanman.ini* File 9-32
9.4. Changing Parameter Values in the lanman.ini File 9-33
9.4.1. Changing Parameter Values with a Text Editor 9-33
9.4.2. Changing Parameter Values using the UNIX program *srvconfig* 9-33

10. Commmand Directory 10-1
10.1. Overview 10-1
10.2. Using net commands 10-1
10.2.1. Administering Supermax LAN Manager/X via the Command Line Net Interface 10-2
10.2.2. From an Enhanced DOS or OS/2 Client 10-2
10.2.3. From the Server Console UNIX System Prompt using the *net* program 10-3
10.2.4. From the Command Line Administration Utility program at the server console 10-4
10.2.5. Abbreviations 10-5
10.2.5.1. Service names 10-5
10.2.5.2. Parameter names 10-5
10.2.6. Using Passwords with Commands 10-5
10.2.7. Using Command Confirmation 10-6
10.3. Command Reference Pages 10-7
10.3.1. Understanding Command Syntax 10-8
10.4. Commands in This Directory 10-9
10.5. Administrative net Commands 10-11
10.5.1. net access 10-12
10.5.2. net admin 10-17
10.5.3. net audit 10-19
10.5.4. net config server 10-22
10.5.5. net continue print 10-27
10.5.6. net device 10-29
10.5.7. net error 10-32
10.5.8. net file 10-35
10.5.9. net group 10-37
10.5.10. net load 10-40
10.5.11. net pause print 10-42
10.5.12. net print 10-44
10.5.13. net save 10-52
10.5.14. net send 10-54
10.5.15. net separator 10-56
10.5.16. net session 10-58
10.5.17. net share 10-61
10.5.18. net statistics 10-69
10.5.19. net status 10-71
10.5.20. net user 10-72

Appendix A. Managing Share-Level Security A-1
A1. What Is Share-Level Security? A-1
A1.1. Passwords A-1
A1.2. Access Permissions A-1
A1.3. Access to Resources Under Share-Level Security A-2
A1.4. Administrative Differences A-2
A1.5. Sharing Resources A-3
A1.6. Sharing the Special Administrative Resources A-3

A2. Setting Up Share-Level Security A-4
A2.1. Planning the Server Setup A-5
A2.2. Configuring the Server for Share-Level Security A-5
A2.3. Starting the Client Program A-6
A2.4. Logging On As the Administrator A-6
A2.4.1. Equivalent net Command A-6
A2.5. Sharing Directories A-6
A2.5.1. Equivalent net Command A-9
A2.6. Setting Up Shared Print Queues A-9
A2.7. Managing Resources A-9
A2.7.1. Looking at Passwords and Access Permissions . . . A-9
A2.7.2. Equivalent net Command A-12
A2.8. Changing Access Permissions A-12
A2.8.1. Changing Passwords A-12
A2.8.2. Equivalent net Command A-16
A2.9. Clearing or Changing the Administrative Password using the net Command A-16
A2.10. Assigning Remote UNIX System Process Execution Privileges A-16
A2.10.1. Procedure A-16

Appendiks B. Managing Logon Validation B-1
B1. Overview B-1
B2. What Is Logon Validation? B-1
B2.1. Centralized Logon Validation B-2
B2.2. Distributed Logon Validation B-2
B2.3. Logon Scripts B-3
B3. Setting Up Logon Validation B-4
B3.1. Changing a Logon Validator's Servername B-5
B3.2. Setting Up Centralized or Distributed Logon Validation . . . B-5
B3.2.1. Setting Up User-Level Security B-6
B3.2.2. Starting the Netlogon Service B-6
B3.2.3. Preparing Clients B-6
B4. Maintaining Logon Validation B-8
B5. Managing Logon Scripts B-8
B5.1. Using Logon Scripts B-8
B5.2. Creating Logon Scripts B-9
B5.2.1. DOS Batch Files or OS/2 CMD Files B-9
B5.2.2. Programs (Executable Files) B-10
B5.2.3. LAN Manager Profiles B-10
B5.2.4. Equivalent net Command B-13

1. Introduction

1.1. Overview

This guide, *System Administrator's Guide*, explains how to administer a local area network (LAN) server that is running the Dansk Data Elektronik A/S Supermax LAN Manager/X Server Program.[1] The guide is intended for an administrator who needs to set up, configure, or administer a Supermax LAN Manager/X server.

Use this guide with the *Supermax LAN Manager/X - User's Guide*, which introduces basic networking terms and concepts, and provides procedures for accessing and using the resources of a LAN Manager server.

1.2. What's in This Guide?

Depending upon your experience and the task you wish to perform, you will not need to read every page of this guide. Table 1-1 discusses the content of each chapter in this guide. Use Table 1-1 below to locate the information you need.

Table 1-1. What to Read	
If you want to...	**Then read...**
learn about the Server Program's features	Chapter 2, *Understanding the Server Program*
find instructions for the user interfaces you will see when administering the server	Chapter 3, *Using the Administrative Interfaces*
configure a server to run user-level security	Chapter 4, *Setting Up A User-Level Security Server*
manage day-to-day server operations	Chapter 5, *Managing Server Operations*
define user-groups and grant access permissions to individual users	Chapter 6, *Managing Users and Groups Under User-Level Security*
create or configure shared directories and disk resources	Chapter 7, *Managing Shared Directories*
create or configure shared printer resources	Chapter 8, *Managing Shared Printers*
fine tune a server's configuration to meet the needs of the LAN	Chapter 9, *Changing the Default Server Configuration*

[1] The Dansk Data Elektronik A/S Supermax LAN Manager/X Server product incorporates version 1.0 of Microsoft® OS/2® LAN Manager technology.

Table 1-1. What to Read	
If you want to...	**Then read...**
learn about the net commands that can be used from the server and understanding their syntax, purpose, and parameters	Chapter 10, *Command Directory*
configure a server to run share-level security	Appendix A, *Managing Share-Level Security*
configure the method by which logon validation is performed	Appendix B, *Managing Logon Validation*

Important
The current release of Supermax LAN Manager/X does not support OS/2 clients.

The separate *Supermax DOS Client Print* product must be installed to support the client print facility for DOS PCs.

1.3. Prerequisites for Administering LAN Manager

Before using the information in this guide, you should perform the following tasks:

1. Install network hardware in computers that will be part of the LAN. (For more information about installing network hardware, see the documents included with your network hardware).

2. Install the LAN Manager Server Program (hereafter referred to as the Server Program) on computers functioning as servers on the LAN. (For more information about installing the Server Program, see *Supermax LAN Manager/X - Client Installation Guide.*)

3. Install either an Enhanced DOS or an OS/2 version of the LAN Manager Client Program (hereafter referred to as the Client Program) on a single computer that is connected to the LAN. You will use this computer to set up and administer the server. Once the server has been set up, other clients can be installed and connected to the LAN. (For more information about installing the Client Program, see *Supermax LAN Manager/X - Client Installation Guide.*)

If you have not completed the tasks outlined above, do so now in the order specified (using the appropriate guides, as indicated).

1.4. Conventions Used in This Guide

Typographical conventions are used in this guide to distinguish certain kinds of information. For example, one convention represents text displayed on your screen; another one indicates information you type at your keyboard. A description of each convention follows.

* Text displayed on your screen is shown in this guide like this:

```
The system is down.
Reboot the system now.
```

  Screen text may be a prompt, a field name, a menu item, an error message, or any other information displayed by the program.

* Information you type at your keyboard is shown in this guide like this:

```
net use drive-ID: \\servername\sharename
```

  You type characters printed in bold lowercase exactly as shown; you replace words printed in light lowercase with terms appropriate to your network. For example, if you want to use the **net use** command to create a link via the *d:* drive to the *util* directory on a server named *yourserv.serve*, you would type:

```
net use d: \\yourserv.serve\util
```

  You can type a command at your keyboard using either uppercase or lowercase letters.

* Keys on your keyboard are shown like this: CTRL .

  When you need to press and hold one key, then simultaneously press other keys, the key symbols are connected by a hyphen. For example, CTRL-D indicates that you press CTRL and D at the same time.

  The carriage return key, used to execute many commands and menu selections, is shown like this: RETURN.

2. Understanding the Server Program

2.1. Overview

This chapter contains the following information:

* A brief description of the basic capabilities that the Server Program offers to the server administrator.

* An overview of the features the Server Program uses to prevent unauthorized access to the LAN or to resources offered by the server.

* A description of the tasks performed by administrators when managing a LAN.

This chapter provides an overview of these topics; complete information concerning these topics appears in later chapters of this guide.

2.2. Server Program Features and Services

This section provides a brief summary of the features and services available with the Server Program.

2.2.1. File and Print Services

The Server Program enables a computer running the UNIX operating system to provide file and print services to DOS or OS/2 computers running the Client Program.

* The file service allows users working at their clients to create, store, and access files on the server's hard disk. These files can be application programs or data files.

* The print service allows users to send print jobs to printers that are connected to other computers on the network. These printers can be connected either directly to the server or to specially configured clients. For more information, see *Shared Client Printers*, below.

2.2.2. Remote Administration

The Server Program allows you to administer the server from either an Enhanced DOS or an OS/2 client running on the LAN, using either a full screen or a command line-oriented administration program. You can also administer the server from the UNIX system by using the Command Line Administration Utility accessed locally at the system console or remotely using a terminal emulator.

2.2.3. Shared Client Printers

In addition to printers connected directly to the server, the Server Program allows users to access network printers that are connected to specially configured Enhanced DOS clients. This is a special option which should be ordered as a separate product.

This feature

* increases the maximum number of network printers beyond the number of physical printer connections available on the server.

* improves network flexibility by allowing a client printer, shared among a common workgroup, to be installed in a location convenient to that group.

2.2.4. Network Message Service

The Network Message service allows the Server Program or other installed applications to send messages to clients.

Messages can be sent from:

* The system console at the server

* Basic DOS clients

* Enhanced DOS clients

* OS/2 clients

Messages can be received by:

* Basic DOS clients

* Enhanced DOS clients

* OS/2 clients

These messages pop up in a special message window that appears in front of any application running on the client. Users can either close the message window manually (with a single keystroke) or allow the message window to time out automatically and close itself.

Some messages can be generated automatically by the Server Program, including network error messages, resource status messages, and print job completion messages. The administrator may wish to send messages to advise users of events on the system, such as an unscheduled server shutdown.

2.2.5. Audit Trail

The Audit Trail provides basic tools to monitor network performance and server resource usage. The Audit Trail feature available only on servers running user-level security provides the following information about each client-to-server link:

* the name of the server resource being accessed

* the type of operation performed or attempted

* the date and time of operation

* the username requesting access

The information generated by the Audit Trail can be used to charge network users for use of server resources. This ability is valuable where billing is done on a per project basis, in an engineering or law firm, for example.

The Audit Trail records past usage of the server. Whenever a connection is opened to a resource that is being audited, the Audit Trail records the opening of the connection; it does not record subsequent actions involving the resource. For example, when a network user reads a file that is being audited, the initial read is recorded. Subsequent reads are not recorded. Thus, the Audit Trail keeps track of initial connections to server resources over a period of time.

Complete instructions for displaying the Audit Trail and turning the Audit Trail on and off appear later in this guide.

2.2.6. Text File Translation

The **ud** command enables users to translate ASCII text files from DOS or OS/2 format to UNIX system format and vice versa. This allows a single text file to work with DOS, OS/2, or UNIX operating system environments and applications. With this capability, users can edit text files by working with familiar text processing tools without the necessity of retraining.

2.2.7. DDE-Term Terminal Emulation

With the DDE-Term terminal emulator, network users at basic DOS or Enhanced DOS clients can directly access the multi-tasking UNIX operating system. This access includes the ability to perform system administration.

2.2.8. Remote UNIX System Process Execution

The **uexec** command provides access to non-interactive UNIX system commands without logging on to the UNIX system and without compromising UNIX system security features. (A non-interactive command is one that does not require you to respond after you first enter it, e.g. the **ls** command). With **uexec**, a user working at a client can execute a non-interactive UNIX system command or series of commands on the server and receive the output back at the client.

The **uexec** command works differently than terminal emulation, which in effect turns the client into a terminal. Instead, remote UNIX process execution can be executed from the DOS command line (on Basic DOS or Enhanced DOS clients) or the DOS compatibility box (on OS/2 clients), maintaining the full functionality of your client.

2.3. LAN Manager Resource Security

This section describes the Server Program's network and server security features. As an administrator, you have to make decisions about who should and who shouldn't be able to use server resources. Under LAN Manager, there are two ways of controlling access to the server's resources:

* Under *user-level security*, you specify what resources each user can access and the type of operations they can perform on each resource. This security mode provides the most stringent security and should be used with most networks. It furnishes exact control over every aspect of user access, and is best for sites with a wide variety of users with differing needs.

  User-level security is the default configuration of the Server Program. Setup procedures for a server running user-level security appear in Chapter 4, *Setting Up A User-Level Security Server*.

* Under *share-level security*, you assign a password to each resource and then control access by giving the password only to users who need the specified resource. Share-level security provides more general control than user-level security, and may be appropriate for sites that are using other LAN products in addition to the Server Program.

  Setup procedures for a server running share-level security appear in Appendix A, *Managing Share-Level Security*.

Every server on your LAN must be running either user-level or share-level security. You may have both user-level and share-level servers on the same LAN. Once it has been established, you should not change a server's security mode.

User-level security mode is required if you wish to use the logon validation or Audit Trail features of LAN Manager.

2.3.1. Logon Validation and Scripts

Logon validation checks a user's password before allowing the user to access the LAN. To use this feature, you need to set up user accounts, clients, and servers for logon validation. To enable logon validation on a particular server, you must do the following:

* Make sure that the server name is no more than 13 characters long (including the *.serve* extension). However, if the server has logon validation enabled, the maximum servername length is 13 characters (including the *.serve* extension).

  For information on changing servernames, see Appendix B, *Managing Logon Validation*.

* Set the value of the *netlogon=* parameter in the *[lmxserver]* section of the server's *lanman.ini* file.

By default, this parameter is set to *no*, disabling logon validation on the server. If you want to use logon validation, you must change the value of this parameter to yes (for complete instructions, see Chapter 9, *Changing the Default Server Configuration*.)

* Make sure that the server is running user-level security.

  Servers performing logon validation must be running user-level security. Other servers on the network that are not performing logon validation may be running either user-level or share-level security (servers can only run one security mode at any given time).

Note: If you choose not to enable logon validation, the server's shared resources are still protected by user-level or share-level security.

If you decide to enable logon validation, you must choose between the two logon validation modes, *centralized* and *distributed*:

* Under centralized logon validation, a designated server validates user requests for access to the LAN.

* Under distributed logon validation, the responsibility for validating usernames and passwords is divided among multiple servers.

Both logon validation modes require users to enter their usernames and passwords to gain access to the network.

The type of logon validation mode used by the network is determined by the value of the *centralized=* parameter in the *[netlogon]* section of the server's *lanman.ini* file. By default, this parameter is set for distributed logon validation. If you want to use centralized logon validation, you must change the value of this parameter (for complete instructions, see Chapter 9, *Changing the Default Server Configuration*).

Logon validation also allows you to configure the working environments of individual users by using *logon scripts*. Logon scripts are batch files that are run whenever the user logs on. These scripts can automate certain LAN Manager tasks, such as making connections to the most frequently used server resources, or invoking a batch file.

For complete information about logon validation and scripts, see Appendix B *Managing Logon Validation*.

2.4. The Administrator's Role

Administration of any network involves designing, setting up, and maintaining the network. This section describes these responsibilities, and divides them into four categories.



Network Design and Installation
The administration of a network begins well before the first directory is shared and continues throughout the life of the network. Some examples of basic administrative tasks are:

* Determining network layout and design

* Creating a naming scheme for network devices and users

* Keeping records for the overall network configuration and network users

* Installing and maintaining hardware and software

* Evaluating new applications and peripherals

These tasks are discussed only briefly in this guide.

Routine Tasks
Several day-to-day tasks are necessary to maintain the network. Some of these tasks are:

* Adding new users and deleting users that no longer need access to server resources. (For more information, see Chapter 4, *Setting Up A User-Level Security Server*, and Chapter 6, *Managing Users and Groups Under User-Level Security*.)

* Setting up shared directories. (For more information, see Chapter 4, *Setting Up A User-Level Security Server* and Chapter 7, *Managing Shared Directories*.)

* Installing applications software. (For more information, see the documentation provided with the application software.)

* Setting up and controlling shared printer queues. (For more information about setting up printers, see Chapter 4, *Setting Up A User-Level Security Server* and Chapter 8, *Managing Shared Printers*.)

* Controlling server disk storage space. (For more information, see Chapter 4, *Setting Up A User-Level Security Server* and Chapter 7, *Managing Shared Directories*.

* Backing up and restoring server files. (For more information, see Chapter 5, *Managing Server Operations*.)

These tasks are performed frequently using various LAN Manager administrative commands.

Troubleshooting Tasks

Certain less frequently performed tasks may be needed because of unexpected or abnormal conditions on the network. These conditions might be caused by such things as faulty wiring, faulty hardware, or overloaded servers. In these cases, the tasks (and solutions) are not as straightforward as the routine tasks. However, aids and diagnostics are available to help find and fix problems. Although the server administrator is often the first contact for users experiencing trouble on the network, you may also need to contact the network administrator to resolve problems.

User Education

Educated users are crucial to a successful network. Key tasks involved in educating network users are:

* Training new network users

* Communicating news about the network to all users

* Providing help to all users

* Maintaining a library of related network documentation for all users.

3. Using the Administrative Interfaces

3.1. Overview

This chapter contains the following information:

* A discussion of the two administrative interfaces available with the Server Program:
  - The Full Screen Net Admin Interface.
  - The Command Line Net Interface.
* A set of procedures for accessing, using, and exiting the Full Screen Net Admin Interface. (It is recommended that you use this administrative interface whenever possible.)

This guide does not provide detailed instructions for using the Command Line Net Interface or **net** commands. Instead, it contains references to appropriate **net** commands, to assist you in locating a description of the command in the proper guide. The **net** commands for administrators appear in Chapter 10. The **net** commands for users appear in the user's guide. These guides included as part of the LAN Manager Server package contain complete information about the Command Line Net Interface and the command syntax for **net** commands.

3.2. The Administrative Interfaces

There are two administrative interfaces available with the Server Program. They are listed below:

* The Full Screen Net Admin Interface, a full-screen, character-based administration program. The Full Screen Net Admin Interface is available only from Enhanced DOS or OS/2 clients.
* The Command Line Net Interface, a DOS-like command-oriented language that uses **net** commands from the DOS or OS/2 system prompt; it is also available from the server console or a client running a terminal emulator. The Command Line Net Interface cannot be used to administer a server from a Basic DOS client.

While it is possible to perform many administrative tasks using the Command Line Net Interface and **net** commands, it is recommended that you use the Full Screen Net Admin Interface, as described in this guide. If you wish to use the Command Line Net Interface and the **net** commands, see the chapter 10 in this guide for the appropriate command syntax.

3.3. Using the Full Screen Net Admin Interface

The Full Screen Net Admin Interface, available only on Enhanced DOS and OS/2 clients, is a full-screen, character-based interface that displays menus of actions and resources. Using the Full Screen Net Admin Interface, you can access interactive menus and dialog boxes that guide you through various LAN Manager tasks. You do not need to memorize commands or syntax to use the Full Screen Net Admin Interface.

When you first start administering a local area network running LAN Manager, you'll probably feel more comfortable using the Full Screen Net Admin Interface for most of your work. Later, when you're familiar with the Server Program and want to start writing batch files to automate administrative tasks, you can begin to learn the command syntax associated with the Command Line Net Interface.

The procedures in this guide use the Full Screen Net Admin Interface to perform most administrative tasks. These tasks also can be performed using the Command Line Net Interface. Following each Full Screen Net Interface procedure, a reference appears for the equivalent **net** commands. For complete information about the Command Line Net Interface, see chapter 10 in this guide.

This section contains the following information:

* Accessing the Full Screen Net Admin Interface
* Working With the Full Screen Net Admin Interface
* Exiting the Full Screen Net Admin Interface

3.3.1. Accessing the Full Screen Net Admin Interface

To access and administer a server by using the Full Screen Net Admin Interface, follow these steps:

1. Log on to the network as *admin* by typing **net logon admin** `password` where `password` is the password associated with the *admin* account on the server you wish to administer.

2. Type **net admin** `\\yourserv` at the client's system prompt, where `yourserv` is the name of the server that you want to administer. Press RETURN. The Full Screen Net Admin Interface background screen appears. The background screen displays information about the current use of the LAN. This screen is your starting point for performing any task using the Full Screen Net Admin Interface. (The background screen is discussed in detail in the next session.) The name of the server being administered is displayed in the *Administering:* field of the background screen. All administrative actions you now perform will affect the server whose name appears in this field.

To access another server without exiting the Full Screen Net Admin Interface, perform these steps:

1. Press the ALT key to highlight the menu bars of the background screen.
2. Select the *View* menu by typing v and pressing RETURN.
3. Use the arrow keys to highlight the *Other server* menu item and press RETURN.

   The *Connect to a Remote Server* dialog box appears.
4. Enter the name of the server you want to administer in the *Servername* text box.
5. Enter the administrative password in the *Password* text box (if different than the one you are currently using).
6. Select the *OK* command button.

   The name of the server being administered is displayed in the *Administering:* field of the background screen. All administrative actions you now perform will affect the server whose name appears in this field.

3.3.2. Working With the Full Screen Net Admin Interface

To perform an administrative task, you select the appropriate menu from the background screen. The menu leads to subsequent menu items which lead to displays called *dialog boxes*. You can use dialog boxes to make selections and/or enter information needed to perform your task.

While working with Full Screen Net Admin Interface, you can press the ESC key to cancel the current operation. To clear all menu items and dialog boxes, keep pressing ESC until only the background screen remains.

You can get help at any time by pressing the HELP function key. Help is available on the background screen in general, and on specific menus, menu items, and dialog boxes. The help information for the background screen also has an index that lets you select help information for a particular topic. If you press HELP while a specific menu or dialog box is on your screen, the information presented is specific to the menu or dialog box.

The following sections describe how to

* understand the background screen.
* use the menus.
* use the dialog boxes.

Instructions are provided for users who have both a keyboard and a mouse and for users who have only a keyboard.

3.3.2.1. Understanding the Screen Display for the Full Screen Net Admin Interface

The background screen appears in Figure 3-1. To access this screen, see the section of this chapter entitled *Accessing the Full Screen Net Admin Interface.*

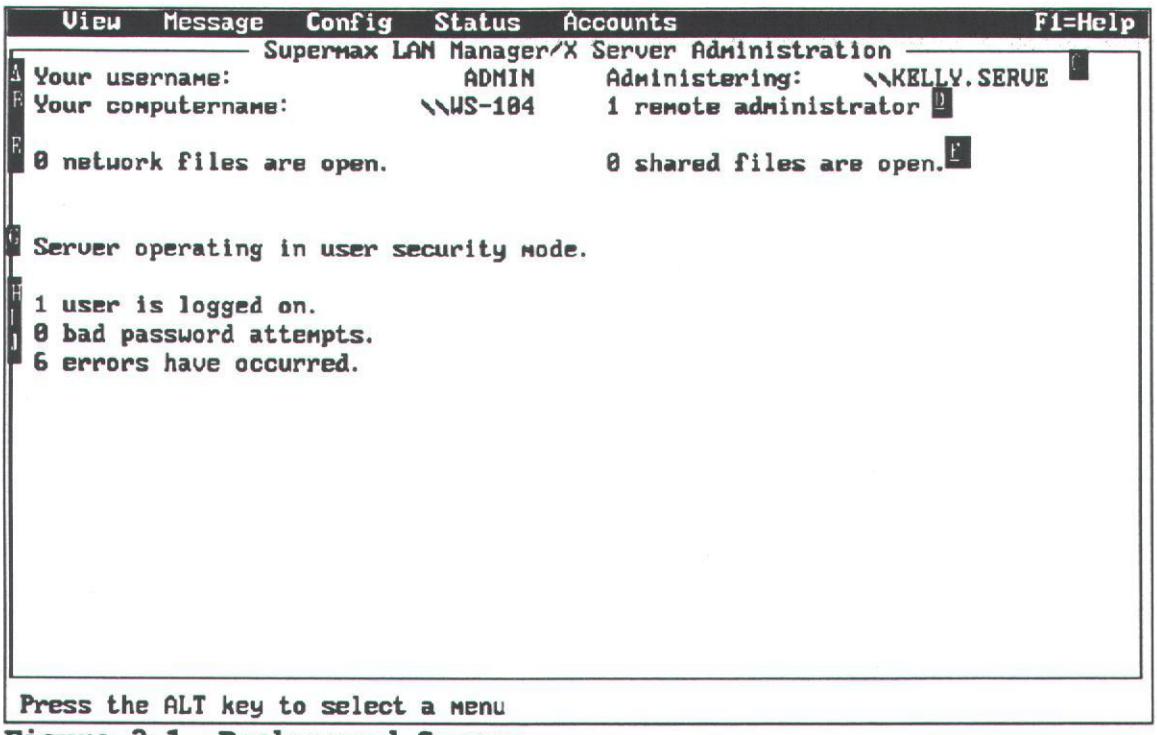


Figure 3-1. Background Screen

The background screen contains the following information:

a) the name you used to log on to the LAN (your username, typically *admin*).

b) the name of your computer on the LAN (your computername).

c) the name of the server you are administering (the servername).

d) the number of users with administrative privileges that are logged on to the server you are administering.

e) the number of files on the LAN you are currently using (on all servers you are linked to).

f) the number of shared resource files currently open on the server you are administering.

g) the resource security mode running on the server you are administering (either user-level or share-level).

h) the number of users currently logged on to the server you are administering.

i) the number of incorrect passwords supplied by users attempting to access resources on the server you are administering (since it was started).

j) the number of LAN errors recorded by the server you are administering since it was started.

Using Menus

The names of the menus associated with the Full Screen Net Admin Interface appear at the top of the display. To perform a task, select the appropriate menu. After you select a menu name, you see a list of menu items. For example, when you select the *View* menu, you see the following (Figure 3-2):

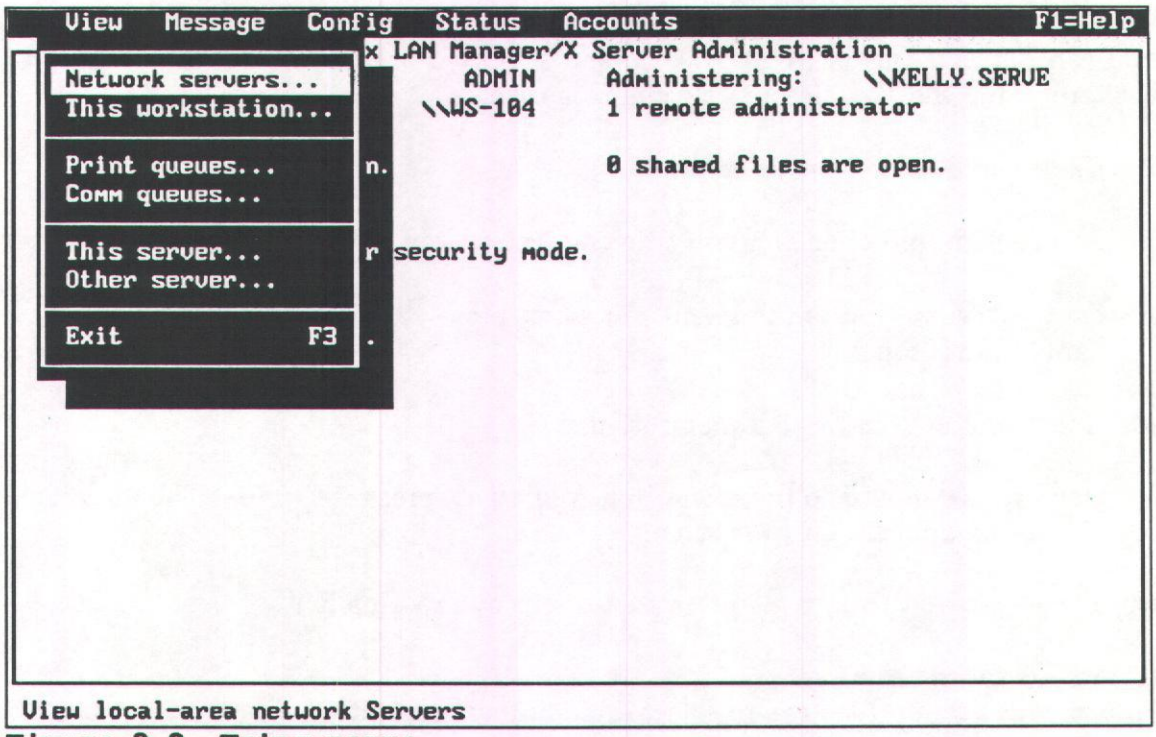


Figure 3-2. Using menus

You perform most tasks through the *View* menu.

There are three methods for selecting menus and menu items:

1. using arrow keys (←, →, ↑, ↓)
2. using accelerator keys
3. using a mouse

Procedures for each of these methods follow.

Using Arrow Keys
To use your arrow keys to select a menu and menu items, follow these steps:

1. Press ALT.

   Because the *View* menu is the first menu on your screen, your cursor is automatically placed at this menu.

You can tell that this is where your cursor is located because, when you press ALT the background of the *View* menu title changes colours.

2. Use ← and → to select a menu.

   The background of each menu title changes as you move around with these keys.

3. Once you've moved to the menu you want, press RETURN or ↓ to see the menu's list of menu items.

4. Use ↑ and ↓ to move to a menu item.

5. Once you've moved to the menu item you want, press RETURN. The appropriate dialog box appears on your screen.

Note: You can exit from a menu or menu item by pressing ESC.

Using Accelerator Keys
To use your *accelerator* keys to select a menu and menu item, follow these steps:

1. Press and hold down ALT to highlight a letter in each menu name.
2. While holding down ALT type the highlighted letter in the name of the menu you want to use (for instance, type v for the *View* menu).

   The menu items for the menu appear under the name of the menu.

3. Still holding down ALT type the highlighted letter of the menu item you want.

The appropriate dialog box appears on your screen.

In some cases, you can move to an area by pressing the accelerator key without also pressing ALT. However, you can always use ALT along with the accelerator key.

Note: You can exit from a menu or menu item by pressing ESC.

Using a Mouse
If you are using a mouse with your client, you can select a menu and a menu item by following these steps:

1. Move the mouse cursor to the name of the menu you want to use.

2. Press and release the left mouse button.

   The menu items for that menu appear under the name of the menu.

3. Move the mouse cursor to the menu item you want and then press and release the left mouse button.

   The appropriate dialog box appears on your screen.

Note: You can exit from a menu or menu item by pressing ESC.

3.3.2.2. Using the Dialog Boxes

Dialog boxes display information and ask you to make selections and enter information. They appear on your screen when you select a menu item from a menu. The information in this section allows you to

* understand the elements of a dialog box
* move around in a dialog box
* use text boxes
* use list boxes
* use check boxes
* use option buttons
* use command buttons
* use display fields

Understanding the Elements of a Dialog Box
Dialog boxes can contain up to six different elements: text boxes; list boxes; check boxes; option buttons; command buttons; display fields.

There are no dialog boxes that you can look at to see all six elements. However, the *Send a Message* dialog box, which contains text boxes, list boxes, option buttons, and command buttons, can give you an idea of how some of these elements can be combined in a dialog box (See Figure 3-3).

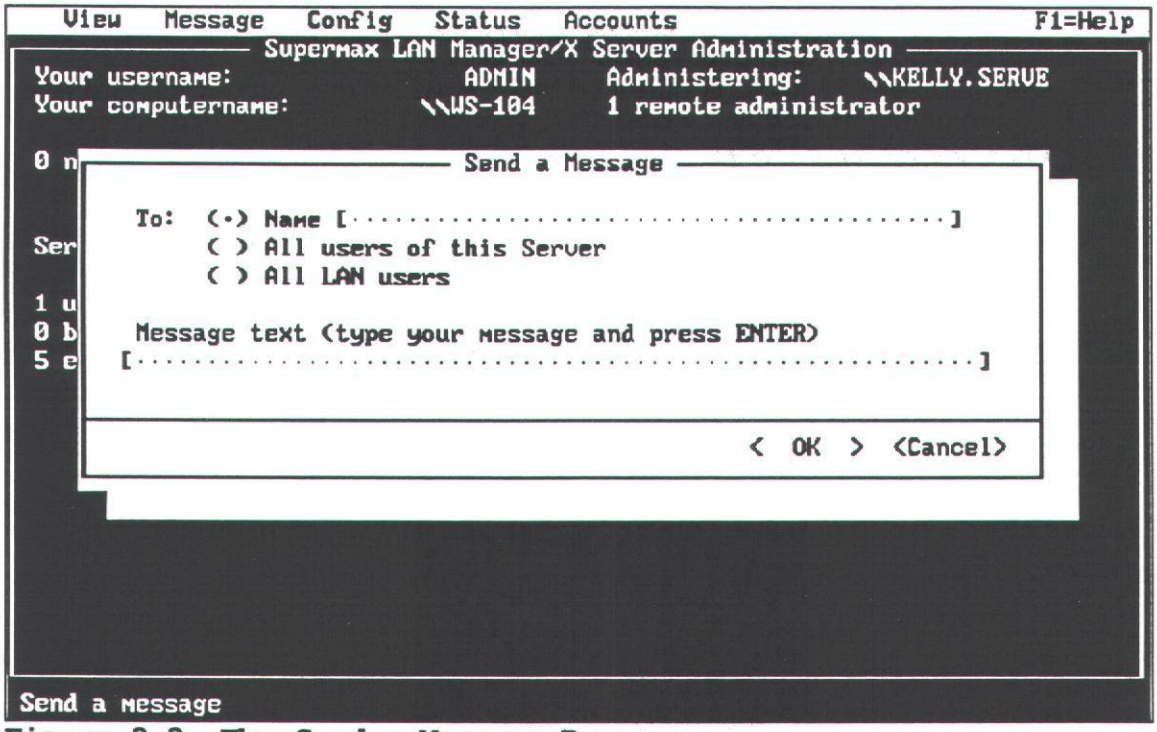


Figure 3-3. The *Send a Message* Box

3.3.2.3. Moving Around in a Dialog Box

You can move from one area to the next in a dialog box using one of the following methods:

* Press TAB to move to the next area in a dialog box. To move backwards, press SHIFT-TAB.

* If you have a mouse, move the mouse pointer to the area you want and press the left mouse button.

* Move between areas using accelerator keys. To use the accelerator keys, follow these steps:

a) Once you are in a dialog box, press ALT.

   A different letter is highlighted or changes color in each area of the dialog box. This is the accelerator key for that area.

b) To move to an area, hold down ALT and press the appropriate accelerator key.

To move around within a dialog box, you can use the TAB key or accelerator keys. Using the TAB key might be easier when you need to move methodically through a dialog box, filling in information as you go. The accelerator keys, in turn, might be more efficient when you need to go to a specific area of a dialog box.

3.3.2.4. Using Text Boxes

Text boxes are areas on the screen where you can enter or change information. Text boxes are surrounded by brackets and contain a series of dots. As you type, you replace the dots with characters. For example,

```
Message text: [I'm leaving for a doct. appt...]
```

Sometimes, text boxes appear with information already filled in. This is the default, or proposed response, for that text box. If you want to use the default information, you can leave the text box as it is.

You can change the contents of a text box using your keyboard or a mouse. Follow the appropriate procedure.

Using Your Keyboard

To fill in or change the contents of a text box from your keyboard, follow these steps:

1. If necessary, move the cursor to the text box by pressing TAB or SHIFT-TAB (to go backwards), or by using the accelerator keys.

2. If necessary, delete any information already in the text box by pressing DELETE or BACKSPACE.

3. Type the desired information in the text box.

   Text boxes can hold more characters than fit in the actual box area on the screen. As you type or move from left to right or right to left, the text box scrolls horizontally to show you its entire contents.

   The edit keys listed in Table 3-1 may help you view or change the contents of the text box:

Table 3-1. Edit Keys for a Text Box

Key	Movement
←	Moves the cursor to the left one space
→	Moves the cursor to the right one space
HOME	Moves the cursor to the first character in the text box
END	Moves the cursor to the last character in the text box

Using a Mouse
To change the contents of a text box with a mouse, follow these steps:

1. Move the mouse cursor to the text box.
2. Press and release the left mouse button.

   A text cursor appears inside the text box.
3. Enter, change, or delete information in the text box.

3.3.2.5. Using List Boxes

List boxes serve two purposes:

* they let you scroll through long lists that wouldn't fit on the screen at one time.
* they present a list of items you can choose from, such as the names of servers or the print requests waiting at a shared printer.

A typical list box looks is shown in Figure 3-4.

If a list box consists of several columns, when you select an item from the list box, you automatically select the entire row in which the item appears.

List boxes are often associated with text boxes; when you select an item from a list box, that item appears in the associated text box.

In Figure 3-5, the user has selected the server *kelly.serve* from the list box. As a result, the associated *Servername* text box contains the servername *kelly.serve*.

You can select an item from a list box using your keyboard or a mouse. Follow the appropriate procedure.

Other drives/dirs List Box (OS/2 clients only)

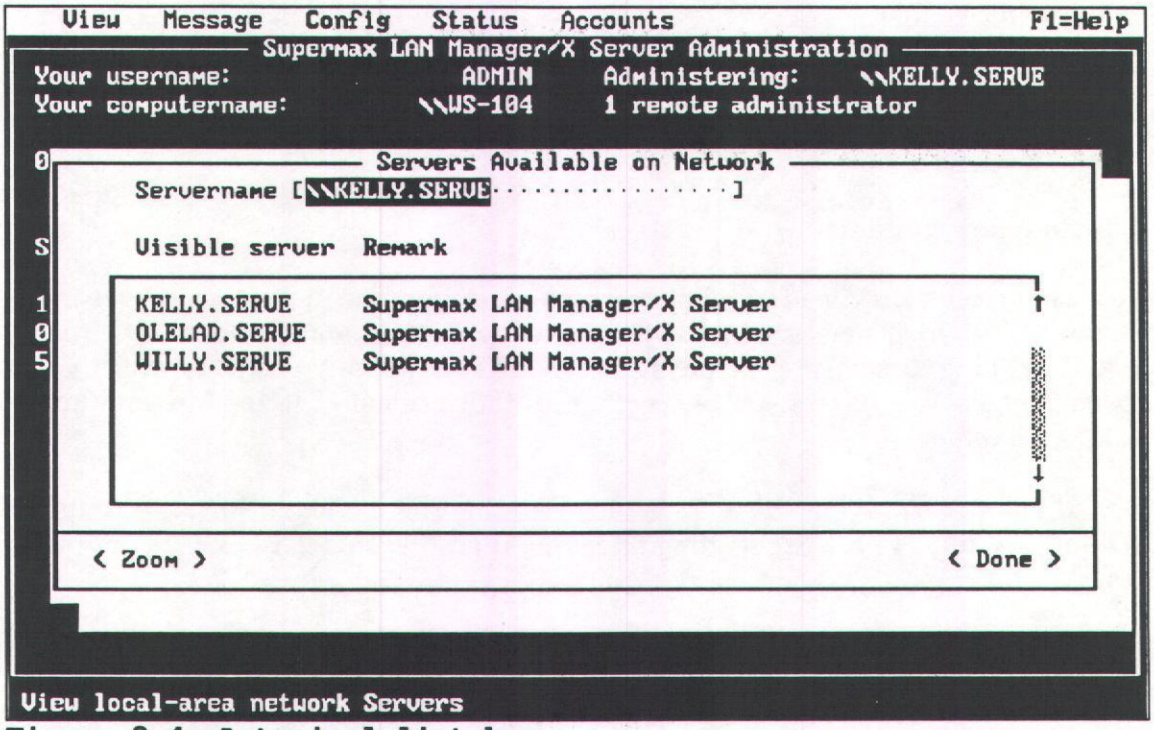


Figure 3-4. A typical list box

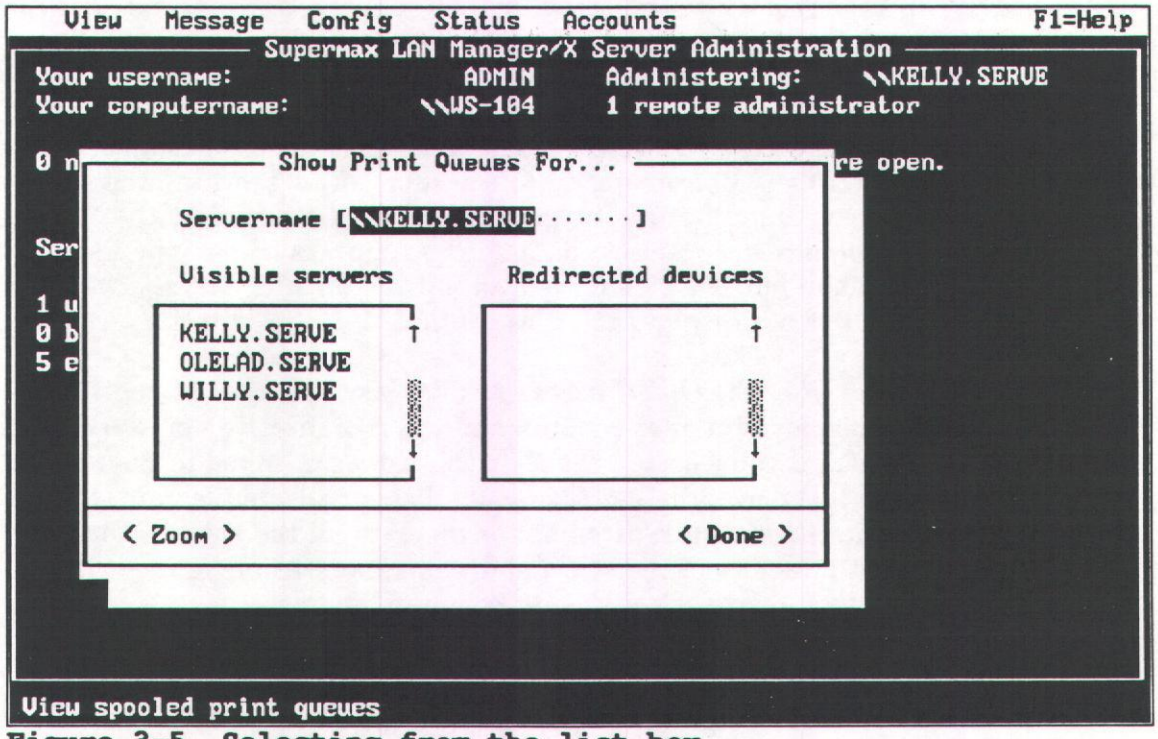


Figure 3-5. Selecting from the list box

The Full Screen Net Admin Interface includes a special list box called *Other drives/-dirs*. This list box appears on your screen when you use the Full Screen Net Admin Interface to

* send a file to another user

* change your message log file (applies to OS/2 clients only)

* load an existing profile

* create a new profile

The *Files in <current directory>* list box lists all of the files in your current working directory. The *Other drives/dirs* list box lists any subdirectories underneath your current working directory, your physical disk drives, and any drives to which you are linked. This list box allows you to specify files that are not contained in your current working directory.

Note: If you are changing the message log file, the File in current directory> list box lists only log files. If you are loading or saving a profile, this list box lists only profile files.

If you select a subdirectory or drive from the *Other drives/dirs* list box, the contents of this list box and the *<Files in current directory>* list box change, as follows:

* If you select a subdirectory, the *<Files in current directory>* list box displays files contained in the subdirectory you selected. In addition, the *Other drives/dirs* list box will display the subdirectories underneath the selected subdirectory, as well as all your available drives. You can select a subdirectory using a keyboard or a mouse. To select a subdirectory using a keyboard, perform the procedure entitled, *Using a Keyboard*, later in this section. To select a subdirectory using a mouse, perform the procedure entitled *Using a Mouse* later in this section. After selecting the subdirectory, select the *OK* command button. If you wish to select a directory that is above your current working directory, select the item that appears as .. in the list box and select the *OK* command button. This moves you up one directory level. The *Files in <current directory>* list box displays the files contained in that directory.

* If you select at drive from the *Other drives/dirs* list box, the *Files in <current directory>* list box displays the files contained in the root directory on the drive you selected. For example, if you selected the *F* drive, and were linked to the shared directory *text* using this drive, the list box would display all the files in the *text* shared directory.The *Other drives/dirs* list box displays all the subdirectories underneath the root directory of the selected drive, as well as all your available drives. After selecting a drive, select the *OK* command button.

Once you have selected the appropriate drive or directory from the *Other drives/dirs* list box, you can select your file from the *Files in <current directory>* list box and select the OK command button to send the file.

Using a Keyboard
To select an item in a list box using your keyboard, follow these steps:

1. If necessary, move the cursor into the list box by pressing TAB or SHIFT TAB (to move backwards), or by using the accelerator keys.

2. Use the keys described in Table 3-2 to move around in the list box. (The contents of an associated text box may change if there are more items in the list than can fit in the list box at one time.)

Table 3-2. Keys Used to Move In a List Box

Key	Movement
↑	Moves the cursor up one line
↓	Moves the cursor down one line
PG UP	Moves the cursor up one page
PG DN	Moves the cursor down one page
HOME	Moves the cursor to the top of a list
END	Moves the cursor to the bootom of a list

The items in a list box are arranged alphabetically. You can move to the first item starting with a particular letter by moving the cursor into the list box and pressing that letter.

3. When you have highlighted the item you wish to select in the list box, press TAB to leave the box. Your item remains selected.

Using a Mouse

To view or select from the contents of a list box using a mouse, follow these steps:

1. Move the mouse cursor to the vertical strip at the right side of the list box. This strip is called a *scroll bar*.

2. Place the mouse cursor over the rectangle in the scroll bar.

   This rectangle is called the *scroll box*.

   The scroll box represents your current location in the list of entries in the list box.

3. Press the left mouse button and hold it down.

4. Move the mouse to slide the scroll box, up or down, to a location in the scroll bar that roughly corresponds to the location in the list box that you want to bring into view.

   When you move the scroll box to the bottom of the scroll bar, you see the bottom of the list. When you move the scroll box to the top of the scroll bar, you see the top of the list. You will usually find the scroll box at the top of the scroll bar when you access a dialog box.

5. Release the left mouse button.

   The list box changes.

6. Move the mouse cursor to your selection in the list box, then press and release the left mouse button.

   The contents of an associated text box may change as you make a list box selection.

3.3.2.6. Using Check Boxes

Check boxes specify options that can be either on or off. By typing an x in a check box, you turn an option on. For example, the following check box suspends message logging at your client:

```
[X] Pause logging messages
```

You can use a check box using your keyboard or a mouse. Follow the appropriate procedure.

Using Your Keyboard

To use a check box from your keyboard, follow these steps:

1. Move to the check box by pressing TAB or SHIFT+TAB (to go backwards), or by using the accelerator keys.

2. Press the Spacebar to place a checkmark in the box or to remove an existing checkmark.

Using a Mouse

To use a check box with a mouse, follow these steps:

1. Move the mouse cursor to the check box.

2. Press and release the left mouse button to either mark or unmark the check box.

3.3.2.7. Using Option Buttons

You use *option buttons* to select from a variety of choices. When you select an option button, a dot appears between the corresponding parentheses. Only one option button in a set can be selected at a time.

A typical set of option buttons looks like this:

```
( ) Disk device
( ) Spooled printer
( ) Communication device
```

To select an option button, follow the appropriate procedure.

Using Your Keyboard
To select an option button from your keyboard, follow these steps:

1. Move the cursor to the set of buttons by pressing TAB or SHIFT TAB (to go backwards), or use the accelerator keys.

2. Use the arrow keys to move the cursor between the individual buttons.

3. When your cursor is placed at the option button you want to select, TAB to the next area in the dialog box. Your option button remains selected.

   When you select a button, a dot appears inside the parentheses. The contents of an associated text box may change when you select an option button.

Using Mouse
To use option buttons with a mouse, follow these steps:

1. Place the mouse cursor within an option button.

2. Press and release the left mouse button.

   The contents of an associated text box may change when you select an option-button.

3.3.2.8. Using Command Buttons

Command buttons perform an action, such as deleting a selected print request from a printer queue or taking you to another dialog box. They appear at the bottom of a dialog box. A typical set of command buttons might be:

```
<OK> <Zoom> <Delete> <Cancel>
```

When a dialog box appears on your screen, one command button is already highlighted. This is the default command button for the dialog box. In some cases, one or more command buttons might be colored-over or faded. These buttons represent actions that you cannot perform at the time.

To choose a command button, perform the appropriate procedure:



Using Your Keyboard

1. Move the cursor to the command button by pressing TAB or SHIFT TAB (to move backwards), or by using the accelerator keys.

2. Press RETURN.

Using a Mouse
To use command buttons with a mouse, follow these steps:

1. Move the mouse cursor to the command button.

2. Press and release the left mouse button.

Special Command Buttons
A few command buttons require special explanation. These are the *Zoom*, *OK* and *Cancel* buttons. You will find these button in many dialog boxes.

The *Zoom* command button moves you to a new dialog box, zooming in on the item you have selected in the current dialog box. When you select an item in a list box for example, a printer queue or a shared resource and then select the *Zoom* button, you zoom in on that item.

The *OK* command button tells LAN Manager that you are ready for the actions or changes you specified in the dialog box to take effect. This button always appears with the *Cancel* command button. You can use the *Cancel* command button to exit a dialog box without saving any changes you made or executing any actions you specified.

3.3.2.9. Using Display Fields

Display fields are areas that only display information. You cannot modify the contents of a display field. A typical display field might look like this:

```
Number of Server sessions started:                    8
Sessions unexpectedly disconnected:                  12
Sessions successfully reconnected:                    1
```

You can distinguish display fields from other areas because the cursor will not move to a display field when you press TAB. Also, there are no accelerator keys for display fields.

3.3.3. Exiting the Full Screen Net Admin Interface

This section describes how to exit from the Full Screen Net Admin Interface and return to the system prompt.

There are two methods for exiting the Full Screen Net Admin Interface:

* To use a function key to exit the Full Screen Net Admin Interface, follow these steps:

1. Close all open menus and dialog boxes by pressing the ESC key as many times as needed.

2. Press the *Exit* function key, F3.

   The client displays the system prompt.

* To use a menu item to exit the Full Screen Net Admin Interface, follow these steps:

1. Close all open menus and dialog boxes by pressing the ESC key as many times as needed.

2. Press the ALT key to highlight the *Main* menus at the top of the screen.

3. Select the *View* menu by typing v.

4. Use the arrow keys to highlight the *Exit* menu item and press RETURN.

   The client displays the system prompt.

3.4. Administering the Server from the UNIX System

3.4.1. Using the Default UNIX System Administrative User Login

The server program provides a UNIX system user login id that should be used when administering the server from a terminal connected to the server. (See Chapter 5.6, *Running the Command-Line Administration Utility*). This UNIX system login is the *lmxadmin* login. The *lmxadmin* login has server administration privileges, but does not have privileges to administer the local UNIX system. This is useful when the server administrator and the UNIX system administrator (*root*) are two different persons, or when you wish to clearly separate the responsibilities of UNIX system administration from those of the server.

4. Setting Up a User-Level Security Server

4.1. Overview

After you have installed the Server Program, you must configure it before users can access shared server resources. This chapter contains the following information to help you configure a server that is running user-level security:

* An explanation of how user-level security works, and the various security issues you need to consider while you set up the server.

* Instructions for identifying and organizing information about users and resources that you will need to configure the LAN Manager server.

* Procedures for enacting the decisions you made when planning the server's configuration.

This chapter contains information and procedures required to configure a server running user-level security. This chapter *does not* contain information on share-level security. For information on setting up servers running share-level security, see Appendix A, *Managing Share-Level Security*.

Note: This chapter *does not* include installation instructions. To install the Server Program, see *Supermax LAN Manager/X - Installation Guide*.

4.2. What Is User-Level Security?

User-level security is one of the two resource security modes available with the Server Program. Servers running user-level security control access to their shared resources by tracking whether a particular user has permission to use a particular resource. Conversely, servers running share-level security control access to their shared resources by determining whether or not a user has the correct password for a particular resource (for more information about share-level security mode, see Appendix A, *Managing Share-Level Security*).

On servers running user-level security, user accounts, user groups, privileges, and access permissions all influence a user's ability to access a particular resource. This section contains information to help you understand how user-level security works, including explanations of

* User accounts

* User groups

* Privileges

* Access permissions

* How LAN Manager determines access to resources.

4.2.1. Understanding User Accounts

A server running user-level security maintains a list of users who can access resources on that server. Each entry in that list is known as an *account* and consists of a username and password. The *username* is the name by which a server recognizes a user. The *password* is a secret code, known only to the user, that verifies the user's identity.

When you add or remove a user from the server, you are actually adding or removing an account. When you change a user's password, you are modifying an account.

Certain user accounts are created automatically when the Server Program is installed. These accounts include *admin* and *guest*.

The *admin* user account is assigned the admin privilege level by default. The system prompts for a password for the *admin* user account during the installation process. This password can be changed at any time.

The *guest* user account is assigned the guest privilege level by default. Users who attempt to access resources on a server on which they do not have a user account are given guest privileges.

Caution: Do not password protect the *guest* user account. When clients are booted, they automatically access their primary servers using the server's *guest* account. If this account is password protected, existing clients will not operate properly, and initial installation for new clients will fail.

4.2.2. Understanding User Groups

For ease in dealing with users, you can define *groups* of users and assign them *groupnames*. Groups simplify server administration when a number of users have similar needs on the LAN. When you need to make a change that affects all users in a group, you do not have to list each of the group's members individually. For example, a group of users who are all members of an accounting department might belong to a group called *acctg*. You can affect the entire accounting department by making a change to the *acctg* group. Although you can add individual users to a group, you cannot add groups to other groups; groups cannot contain other groupnames as members.

Certain groups are created automatically when the Server Program is installed. There are two of these groups: *users* and *uexec*. The *users* group contains all users with user accounts on the server as members; the *uexec* group contains those users who can run UNIX system processes on the server by executing the *uexec* command at their clients (for more information on the *uexec* command, see the *Supermax Lan Manager/X - User's Guide*).

By default, the *admin* user account is a member of both the *users* and the *uexec* groups.

By default, the *guest* user account is a member of the *uexec* group.

4.2.3. Understanding Privileges

Every user's account has an assigned *privilege* level. The privilege level determines the type of actions that a user can perform on the server. There are three privilege levels: *user*, *guest*, and *admin*:

admin Individuals with *admin* privilege can create accounts, assign access permissions for resources, manage device queues, and grant privileges to other users. Any user to whom you grant this privilege level should have the same qualifications and knowledge as you, since that person will have full access to every part of the server. The admin privilege overrides all other access permissions and privileges, so assign it with discretion.

user Individuals with *user* privilege can perform all LAN tasks except those specifically reserved for administrators. Users with user privilege are members of the *users* group. The user privilege level is the one you will assign to most users.

guest The *guest* privilege is the same as the user privilege, except that users with guest privilege are not members of the users group. This lets administrators control a guest's use of the server.

Privileges are associated with user accounts rather than with specific server resources.

To understand the access permissions associated with specific server resources, proceed to the next section, *Understanding Access Permissions*.

4.2.4. Understanding Access Permissions

On the LAN Manager server, users and groups can be permitted (or not permitted) to access a resource.

Users who are not permitted to access a resource, either individually or as a member of a group, will be able to link to that resource, but will be unable to perform any other operations with it.

Users who are permitted to access a resource can have a unique set of *access permissions* associated with that access. Once a user links to a resource, these access permissions control the operations (such as reading, writing, or creating) the user can perform with the resource.

Table 4-1 describes the access permissions that can be assigned to a user or group that is permitted to access a resource.

Table 4-1. LAN Manager Resource Permissions

Resource	Access
Disk	C Create D Delete R Read W Write X Execute A Change Attributes P Change Permissions Y Yes (RWCDA) N No
Shared Print Queue	Y Yes (C) N No

If the resource is a disk area (file storage space on the server's hard disk), you can control whether the user can create new files, delete files, execute programs, or perform other operations by setting the proper combination of access permissions.

If the resource is a shared print queue, you can control whether or not the user can submit a job to that print queue.

As a special case, you can give users the ability to set their own access permissions on selected resources. For example, you might set up a home directory for a user on your server, then give the user the ability to set access permissions on anything within that directory. The user can then control who else can read, write, or modify files in that directory.

4.2.4.1. Disk Resource Access Permissions

A disk resource is a disk drive, a directory, or a file. Access permissions that can be assigned to a user or group with regard to a disk resource appear below:

Create (C) Allows a user to create files and directories within the shared disk resource. The C access permission does not grant read or write access to existing files (each of these operations require their own access permissions). After creating a file, a user can read or write to that file only while it is initially opened. Once closed, the user will be unable to open it again.

Delete (D) Allows a user to delete files and directories within the disk resource (but not to delete the disk resource itself).

Read (R) Allows a user to read or open files and to change directories.

Write (W) Allows a user to write to a file.



Execute (X)

Allows a user to open a file for execution.

Note: If you assign R access permission, you do not need to assign X access permission. If you assign X access permission without R access permission, OS/2 clients can execute the file but not read it, while DOS clients cannot read or execute the file.

Change attributes (A)

Allows a user to change the DOS or OS/2 physical file attributes. These file attributes take precedence over LAN Manager access permissions.

Change Permissions (P)

Allows a user to change the LAN Manager access permissions for the resource.

Yes (Y)

An abbreviation for the RWCDA group of access permissions.

No (N or None)

Prevents a user from doing anything. For disk resources, the N access permission is sometimes indicated by a colon with nothing after it; you do not actually see the letter "N." When you assign this access permission, you cannot assign any other access permissions. Use this access permission to exclude individual users from access despite their group memberships.

For example, if you give read and write access permissions to the *users* group, you can exclude a specific user in the users group by assigning that user the *N* access permission.

The N access permission should not be assigned to groups. When evaluating group access permissions, LAN Manager considers the union of all applicable group access permissions.

For example, if you give RWC access permission on a directory to the users group, but N access permission to the *laser* group, members of the *laser* group could still use the directory if they were also members of the *users* group. Assigning *N* access permission to a group does not guarantee that all users of that group will be denied access to the resource.

The Full Screen Net Admin Interface provides convenient groupings of these access permissions, so that you can easily assign common combinations of access permissions. Some of these commonly used combinations include RWX (read, write, and execute) and RWXCDA (read, write, execute, create, delete, and change attributes).

4.2.4.2. Shared Print Queue Access Permissions

A shared print queue is a server resource that accepts print job requests. A print job request is a collection of data, such as a file, that you send to a queue to be printed. A single server may have many shared print queues, which output print jobs to various printers that are either connected to the server directly, or are connected to other computers on the LAN. Once you have sent a print job request to a shared print queue, you have no further interaction with the queue.

The Server Program allows you to assign access permissions to groups and individual users for each shared print queue. In this manner, you can control who can access the various printers on the LAN.

For each shared print queue, you can assign either of the following access permissions to users or groups:

Permitted Allows the user or group to use a particular printer queue.

Not permitted Prevents a user or group from using the shared print queue.

4.2.5. How LAN Manager Determines Access to Resources

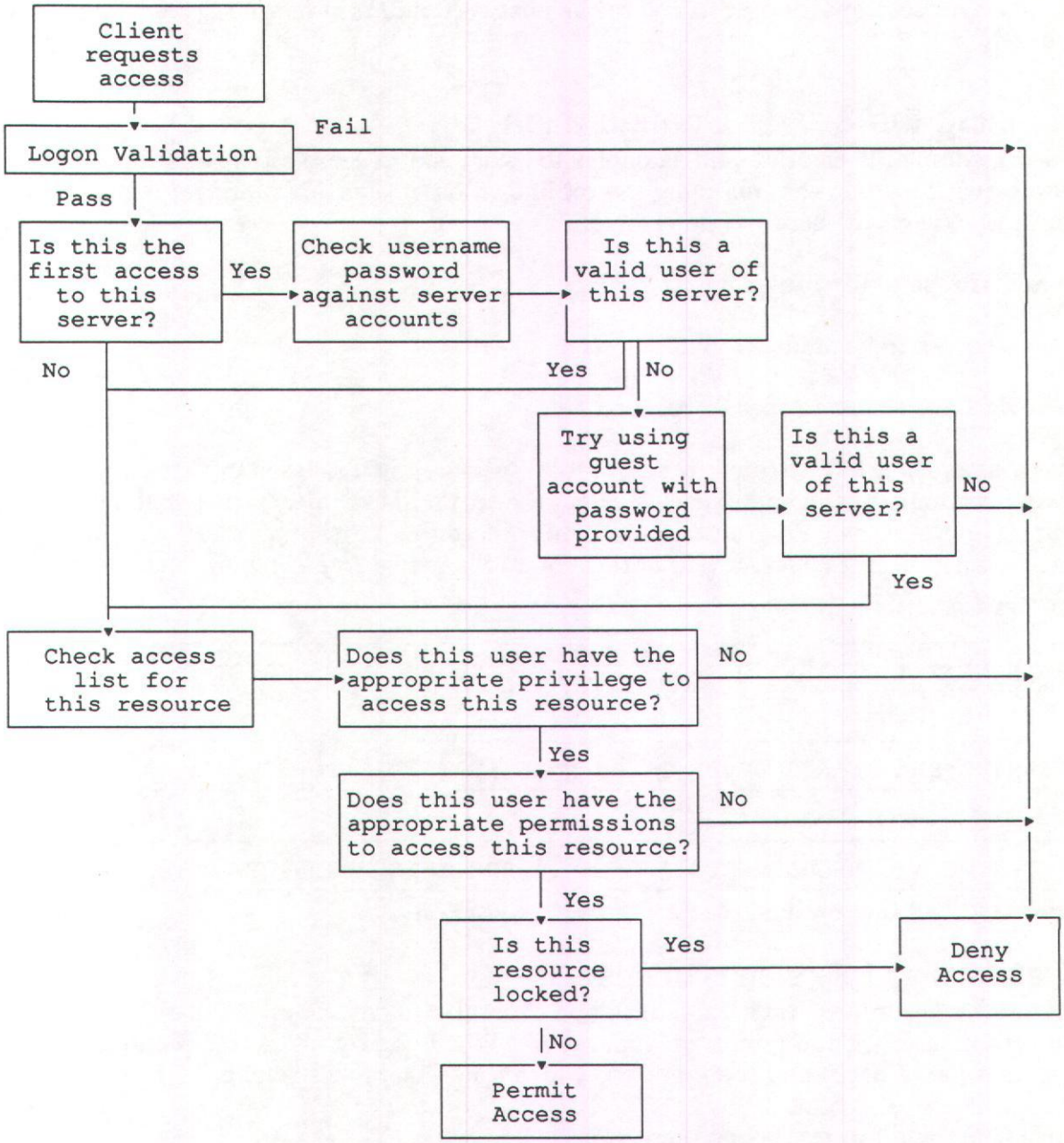
The method used by LAN Manager to determine whether or not a user should be allowed to use a shared resource is illustrated in Figure 4-1. Basically, a user's ability to access and perform operations with a shared resource depends upon three general considerations:

1. Was a valid username and password provided when the user attempted to log on to the network? If so, the user is allowed to link to the resource. If not, LAN Manager attempts to determine the problem. If the username is recognized but the password is not, the user is given the opportunity to re-enter the password. If the username is not recognized, LAN Manager will allow access using the *guest* user account.

2. What is the user's privilege level? If the user has admin privileges, all further operations are allowed. If the user has user or guest privileges, administrative operations are denied, but some other operations can be performed. These operations are determined by the limits of item 3, below.

3. What access permissions does the user have for the resource (either individually or as a member of a group)? If the user has read only access permissions for a directory and attempts to create a file in that directory, the operation will be denied.

In general, the ability to link to a resource does not guarantee that you will be able to perform any desired operations with that resource. In some cases, it may be possible to link to a resource but impossible to perform any meaningful operations with the resource.



Figur 4-1. Access Under User-Level Security

4.2.5.1. Summary of Access Permissions

For each shared disk and shared print queue resource on the server, these decisions must be made regarding user and group access permissions:

1. Should a specific user or group be permitted to access the resource at all?

2. Should unique access permissions be assigned to each user or group that will be permitted to access the resource? If so, what access permissions should be assigned?

After you answer these questions, proceed to the next section, *Planning the Server Configuration*.

4.3. Planning the Server Configuration

This section contains information and examples to assist you in completing the first task of the server setup process planning the configuration of the LAN Manager Server Program. This section will help you determine:

* Users and groups to be created on the system

* Shared resources to be made available to users

* Who should have access to specific resources

These planning steps are illustrated in Figure 4-2. Each step is discussed in detail in the following sections. At the end of each section, there is a list of information that you should supply to the Server Program. Actual input procedures for this part of the setup process are described in the last section of this chapter, entitled *Implementing the Server Configuration*.

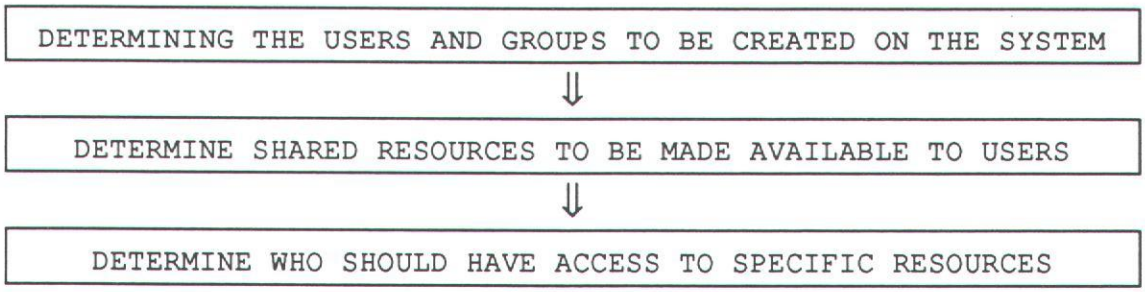


Figure 4-2. Planning the Server Configuration

4.3.1. Determining Users and Groups

This section provides information, guidelines and examples to determine the number and organization of users and groups on your server. When you complete this section, you will have a list of users and the groups to which those users will belong.

To organize users and groups, follow these steps:

1. Determine the number of users who will have accounts on this server.

   If the server being set up is to join an existing network, check with the network administrator to ensure that the addition of new users (or the reorganization of existing users) is distributed evenly across the available servers.

2. Assign each user account a username.

Usernames can be a maximum of 20 characters long and are composed of alphanumeric (a-z, or 0-9) and the following special characters:

$ % - _ @ { } ~ ' ! # ( )

(Do not use special national characters.) Usernames are case insensitive. For example, username *YOURNAME* is the same as username *yourname*.

3. Organize your list of users into groups.

4. Assign each group a groupname. To assign groupnames, you will need the answers to the following questions:

   * Are there users who perform the same types of tasks or functions?

     For example, users who also happen to be members of the same department or workgroup, might be gathered into a group reflecting the departmental or workgroup's purpose, such as an accounting department or a project team.

   * Are there users who, though performing different types of tasks, require the same sorts of server resources?

     For example, the copywriters and commercial artists in an advertising agency require access to shared laser printers. Both copywriters and artists might then be assigned to the same group account for this purpose.

   Groupnames can be a maximum of 20 characters long and are composed of alphanumeric (a-z, A-Z, or 0-9) and the following special characters:

   $ % - _ @ { } ~ ' ! # ( )

   Like usernames, groupnames are also case insensitive.

After you have completed a list of users and groups to create on your server, evaluate the resources that need to be shared by using the instructions in the next section, *Determining Shared Resources*.

4.3.2. Determining Shared Resources

This section provides guidelines and examples help you prepare a list of disk and printer resources to be shared on the server.

To determine the resources to be shared, follow these steps:

1. Answer the following questions:

   * What application software needs to be shared?



For example, a group of accountants might share spreadsheet and word processing applications. An administrator surveying their needs would create two separate shared directories for these applications.

* What data files need to be shared?

  For example, monthly sales figures might be stored in a shared directory created for the accounting department.

* What directories (other than those required for shared applications and data) need to be shared?

  For example, each accountant might be assigned a home directory to provide file storage for data not stored in shared directories.

* What shared print queues need to be created?

  For example, a group of accountants needs access to both laser printers and dot matrix printers. The laser printers are used for word processing. The dot matrix printers are used for spreadsheets. Their administrator would plan two shared print queues: one for laser printers, and one for dot matrix printers.For ease of use and administration, each of the two queues would contain only the appropri ate type of printer (laser or dot matrix).

2. Assign a **sharename** to each shared resource. Sharenames can have a maximum of 8 alphanumeric characters.

   Sharenames should describe the resources they share and should be easy to remember. For example, a shared print queue for laser printers might have the sharename *lasers*. A sharename however, does not have to be identical to the actual name of the resource being shared. For example, a directory containing your word processing files might be contained in the server's */usr2/yourname/wp* directory; but this directory's sharename might be *words*.

4.3.2.1. Default Shared Directories

The Server Program provides the following default shared directories:

ddeadmin — Contains the *PRINTLOG* directory. The *PRINTLOG* directory contains files used to record messages generated by the UNIX system or Message Service whenever a printer fault or error occurs.

util — Contains DOS programs and utilities to use and administer the LAN (this directory is also shared under the sharename *U* for UNC access).



util2	Contains OS/2 programs and utilities to use and administer the LAN (this directory is also shared under the sharename *U2* for UNC access).
users	Contains user home directories. The users' shared directory is created only when logon validation is enabled.

Each of these directories is accessible by all users, regardless of privilege settings (admin, user, or guest); *guest* users, however, have read-only access permissions for these directories. In addition, access to *util* (for Basic DOS and Enhanced DOS clients) and *util2* (for OS/2 clients) is performed automatically by using Universal Naming Convention (UNC) names in each client's *path* statement. At boot time, the client links to the shared directories *U* (for *util*) and/or *U2* (for *util2*) which are UNC names in the path statement. For complete information concerning UNC names and the client's path statement, see *Supermax LAN Manager/X - User's Guide*.

4.3.2.2. Organizing Server Files and Directories

When you share directories on a server's hard disk, it is important for the disk to be well organized. If several people use the same directory for a lot of different projects, the directory will soon be a clutter of unrelated files. You should spend some time creating and sharing separate directories for different groups of users. If each user or group has a well-defined work area on the hard disk, it will be easier to keep files organized.

Before you share directories over the local area network, you should decide how to organize them. Generally, you will be able to organize files into directories related to particular projects or groups of people.

Although it might seem easiest to share an entire hard disk (by specifying its root directory) with everyone on the local area network, it can be a mistake not to anti cipate the organizational and security problems that can result.

Be careful not to share directories that contain sensitive files or programs that should not be accessed by network users. Confidential files should either be stored locally on a client computer or should be accessible only to appropriate users.

4.3.2.3. Recommended Locations for Creating New Shared Directories

When the Server Program is started, default directories (on the UNIX system) are established to function as the location for creating new shared directories (including user's home directories) on the server.

If an administrator attempts to share a directory (or assign a home directory) that does not currently exist, the Server Program will automatically create the new directory, provided it is located in one of these default locations.

Default directories are created in the following file systems:



* Any non-Remote File Sharing (RFS) file system mounted at the */usr/lanman* mount point.

* Any non-RFS file system mounted at a mount point which matches the pattern */usr#/lanman*, where # can be numbers 2 through 9 (for example, */usr2*, or */usr3*).

These directories are assigned the proper ownership and access permissions by the Server Program, so that new directories can be created automatically when necessary. It is recommended that all new shared directories be located in these default locations.

If you attempt to share a directory (and that directory does not already exist as a UNIX system directory) in some other location on the server, the UNIX system will deny access, and the directory will not be created by the Server Program.

You can create additional base directories that will allow creation of new directories during share operations. To create a new base directory on the server, follow these steps:

Caution: Do not use the root directory (/) as an additional base directory. Otherwise, you may exhaust free disk space in the root file system and crash the server's UNIX system.

1. Log in at the server console as *root*.

2. Create the new directory on the server's UNIX system by typing

```
mkdir /filesystem/dirname
```

   where *filesystem* is the file system mount point for the new directory, and *dirname* is the new directory name. Press RETURN.

3. Assign the correct UNIX system permissions to the new directory by typing

```
chmod ug=rwx  /filesystem/dirname
chmod 0=rx  /filesystem/dirname
```

   where *filesystem* is the file system mount point for the new directory, and *dirname* is the new directory name. Press RETURN.

4. Assign the correct UNIX system group name to the directory by typing

```
chgrp DOS----  /filesystem/dirname
```

   where *filesystem* is the file system mount point for the new directory, and *dirname* is the new directory name. Press RETURN.

5. Assign the correct UNIX system owner name to the directory by typing

```
chown lanman /filesystem/dirname
```

where *filesystem* is the file system mount point for the new directory, and *dirname* is the new directory name. Press RETURN.

You can now share the directory by using either the Full Screen Net Admin Interface (for instructions, see *Sharing Directories*, in this chapter), or the Command Line Net Interface (for instructions, see the Chapter 10, *Command Directory* in this guide).

Example
You need to create a new directory for spreadsheet files. You have decided to name this new directory *spreads*. You want to locate this directory in the */apps* UNIX system directory on your server, since this is the directory containing all of your spreadsheet programs.

You log in at the server console as *root*. To create the new directory, you type **mkdir /apps/spreads** and press RETURN. To assign the proper UNIX system permissions, you type **chmod ug=rwx, o=rx /apps/spreads** and press RETURN. To assign the proper UNIX system group, you type **chgrp DOS---- /apps/spreads** and press RETURN. To assign the proper UNIX system ownership, you type **chgrp lanman /apps/spreads** and press RETURN.

To share the directory from either an Enhanced DOS or OS/2 client, start the Client Program and log on to the network as a user with administrative privilege (in this case, you use the *admin* username). You use the Command Line Net Interface to share the directory by typing

```
net share spreads=c:/apps/spreads /users:6
```

and pressing RETURN. Then you specify that the *users* group should be able to access the shared directory, by typing

```
net access c:/apps/spreads /add users:r
```

and pressing RETURN.

The *spreads* directory is now shared on the network and available to members of the *users* group.

Caution: Do not use the root directory (/) as an additional base directory. Otherwise, you may exhaust free disk space in the root file system and crash the server's UNIX system.

4.3.3. Determining Access to Resources

This section provides information, guidelines, and examples for setting up the default user-level security mode on a server. When you complete this section, you will have two lists for each shared resource on the server:



* The first list will contain those users and groups allowed access to a particular resource. If the resource is a disk resource, the list will also contain the user and group access permissions for the resource.

* The second list will contain users and groups who are denied access to this particular resource.

Careful planning at this point will improve the server's security and overall effectiveness.

To determine access to server resources, answer the following questions:

* Which directories and files should be available to some users and groups but not others?

  For example, your corporation's controller might have access to a shared directory containing payroll information for the corporation's employees. This same controller might also have access to a shared directory containing the corporation's sales figures. These sales figures and the shared directory containing them might also be accessible to the company's sales representatives. But you may elect to prevent the sales representatives from accessing the directory containing employee payroll data.

* Should users with access to certain files and directories be permitted to revise or delete them?

  For example, accountants and sales representatives might both have access to a shared directory containing sales and commission figures. But while the accountants can revise and update sales and commission files, the sales representatives can only read these files.

* Should certain shared print queues be available only to specified groups?

  For example, members of a word processing group might have access to shared print queues of high speed laser and dot matrix printers. Members of the shipping and receiving department may only have access to shared print queues for dot matrix printers.

After you have developed your lists of users and the resources accessible to them, continue with the next section, *Implementing the Server Configuration*.

4.4. Implementing the Server Configuration

This section provides instructions for entering the configuration information into the LAN Manager Server Program (this configuration information was identified in the previous section, *Planning Your Server Configuration*). To implement the server configuration, you will need to perform the following tasks:

* Start the Client Program
* Log on as the administrator
* Set up logon validation (optional)
* Set up the Alerter service (optional)
* Set up resource auditing (optional)
* Create new user groups on the server
* Create new user accounts on the server
* Share directories
* Configure printer ports for printers connected to the server (if necessary)
* Create shared printer-queues
* Create common user startup operations
* Create a turnkey environment (optional)

This sequence of tasks is illustrated in Figure 4-3. Instructions for performing each of the tasks appear in the following sections.

4.4.1. Starting the Client Program

Before you can start the Client Program, it must have been installed on either your computer's hard disk or a Client Boot Diskette (for complete information concerning installing the Client Program, see *Supermax LAN Manager/X - Client Installation Guide*).

Note: To administer the server, you must be running either the Enhanced DOS or the OS/2 version of the Client Program.

To start the Enhanced DOS version of the Client Program, type:

```
lmxe
```

and press RETURN.

4.4.2. Logging On as the Administrator

After starting the Client Program, you must log on to the server you want to administer. When you log on, you must log on as a user with administrative privilege (such as *admin*) on that server.

To log on to a server as an administrator, follow the instructions in the section entitled *Accessing the Full Screen Net Admin Interface*, in Chapter 3.

Example
You want to perform some administrative tasks on the *print2.serve* server down the hall. Rather than walk to the *print2.serve* server, you decide to administer the server from your client. Because you are not logged on as *admin* and your user account on the *print2.serve* server does not have administrative privilege, you must log on to that server as *admin*.

You log on to the network by typing **`net logon admin`** `password` at the client's system prompt (replacing *password* with the appropriate password for *admin*). Then you press RETURN.

You invoke the Full Screen Net Admin Interface and identify *print2.serve* as the server you intend to administer by typing **`net admin \\print2.serve`** and pressing RETURN. The *Administering* display field of the Full Screen Net Admin Interface shows the *\\print2.serve* servername. This verifies that you are now administering the *print2.serve* server.

When you have logged on, you can complete any of the next three tasks which are optional, or proceed to section 4.4.6, *Creating New User Groups*, p.4-19).

4.4.3. Setting Up Logon Validation

Logon validation is an additional (and optional) feature, available only with servers running user-level security. With logon validation, users must supply their username and secret password before they are allowed to access the LAN.

Logon validation offers the following benefits:

* Provides increased security to prevent unauthorized users from accessing the LAN

* Allows a common set of logon scripts to be executed by all users accessing a centralized logon server

The following checklist summarizes what you must do to make logon validation work on your network:

1. Make sure that any server that will act as a logon validator has a servername of no more than 13 characters (including the *.serve* extension).

   If the length of a logon server's name is greater than 13 characters, users may receive the following error message when they try to start the Enhanced DOS Client Program:

   ```
   NET2124: Insufficient memory
   ```

If your server is not performing logon validation, the maximum length for the servername remains 14 characters. For more information on changing servernames, see Appendix B, *Managing Logon Validation*.

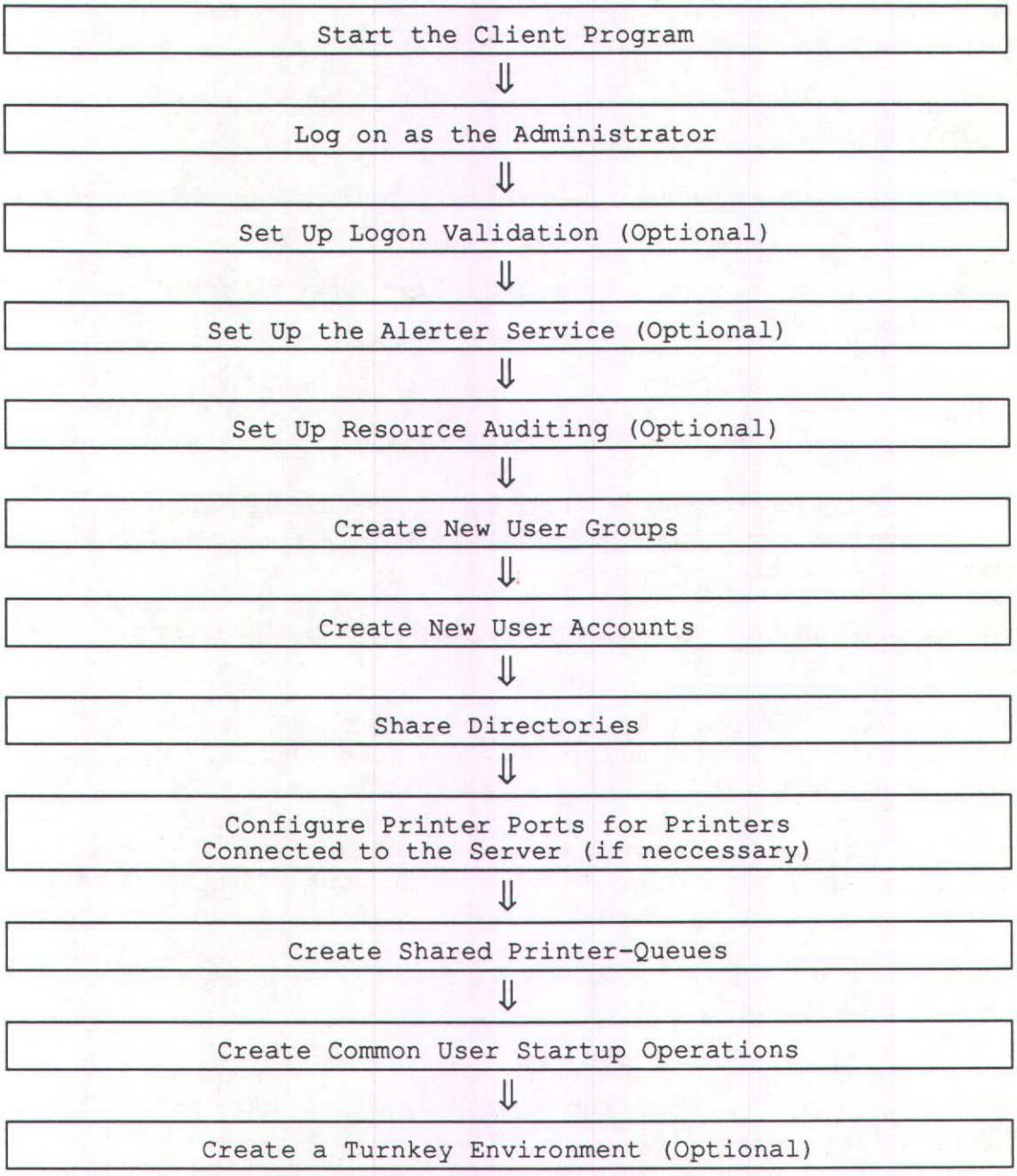


Figure 4-3. Implementing the Server Configuration

2. Specify whether the LAN will use centralized logon validation (one server in the LAN group validates all logon requests) or distributed logon validation (more than one server in the LAN group validates logon requests).

   To do this, set the *centralized*=parameter in each server's *lanman.ini* file to the appropriate value (either *yes* or *no*):

   * For centralized logon validation, all servers in the LAN group should have this parameter set to *yes*.

   * For distributed logon validation, all servers in the LAN group should have this parameter set to *no*.

   To set the value of the *centralized*=parameter, see Chapter 9, *Changing the Default Server Configuration*.

3. Set up user-level security on each server that is to be a logon validator. If centralized logon validation is used, one (and only one) server must be a logon validator. If distributed logon validation is used, more than one server can be a logon validator.

   Then, for each server that will be a logon validator, enable the *netlogon*=parameter in the server's *lanman.ini* file. For complete instructions, see Appendix B, *Managing Logon Validation*.

4. Prepare all clients for logon validation. For complete instructions, see Appendix B, *Managing Logon Validation*.

5. Maintain logon validation by keeping track of user accounts, properly installing and configuring new servers, and providing logon scripts. For complete instructions, see Appendix B, *Managing Logon Validation*.

For complete instructions on how to set up logon validation on your LAN, proceed to Appendix B, *Managing Logon Validation*. Then return to this chapter and continue the tasks for implementing the server configuration.

If you do not wish to set up your server as a logon validator, continue with the next section, *Setting Up the Alerter Service*.

4.4.4. Setting Up the Alerter Service

The Alerter service is an additional (and optional) feature, which can be configured to send automatic alert messages to selected usernames when certain problems occur. When configured, the Alerter service is started automatically, and cannot be stopped.



You enable and configure the Alerter service by setting the values of various parameters in the server's *lanman.ini* file. To specify which users should receive alerts, you use the *alertnames*=parameter. With the *alertthresh*=parameter, you can specify the time intervals (frequency) at which certain types of alerts are generated. For instructions on setting the values of these parameters, see Chapter 9, *Changing the Default Server Configuration*.

The Alerter service sends messages to specified usernames under the following conditions:

* Excessive errors have occurred
* Excessive bad password attempts have occurred
* Excessive bad access attempts have occurred
* The Audit Trail file is full
* The error log file is full
* A printer is out of paper
* A printer is malfunctioning
* A print request has been deleted
* A print request has completed

In the first three conditions listed above, you can control the time interval at which alerts are sent. See Chapter 9, *Changing the Default Server Configuration*, for information about setting the values of the following parameters in the server's *lanman.ini* file:

* *erroralert=* for error alerts.
* *logonalert=* for excessive bad password attempts
* *accessalert=* for excessive bad access attempts
* *alertthresh=* for how often alerts of any kind will be sent

4.4.5. Setting Up Resource Auditing (Audit Trail)

The Audit Trail is an additional (and optional) feature, available *only* on servers running user-level security. For each resource being audited, the Audit Trail records when the resource was accessed, who accessed it, and what was done with it. You can turn the recording of audit information on and off, for all shared resources or for specific shared resources.

When you start the server, its ability to record audit information is determined by the value of the *auditing=* parameter in the server's *lanman.ini* file (see Chapter 9, *Changing the Default Server Configuration*, to set this parameter's value). If this parameter is set to no when the server is started, audit information cannot be recorded for any shared resource on the server.

However, if the server was started with the *auditing=*parameter set to *yes* you can control auditing for each shared resource. When you share a resource, you are asked to specify whether or not the Audit Trail should be enabled for the resource. Regardless of your answer, it is possible to turn auditing for the resource on or off at any time thereafter.

The Audit Trail records only the opening of connections, not subsequent actions that involve the resource. For example, individual reads to a file are not recorded, only the initial open.

Because the Audit Trail records audit information on every opening of a file, some applications may generate a large number of audit entries during normal operation. If you find that an application is generating too much audit information, you can take either of two actions:

* Turn auditing off for the resource

* Turn auditing on only for a specific file in the application's directory, leaving auditing off for the other files. You may have to experiment to find out which file or combination of files will give you the desired amount of audit information.

To display the Audit Trail, see the instructions in Chapter 5, *Managing Server Operations*.

4.4.6. Creating New User Groups

Before creating any new user accounts on the server, you should create any new user groups you will need. Then, when you create new user accounts (instructions appear in the following section), you will be able to assign them to membership in the appropriate groups.

Before performing this procedure, you should have a list of new user groups to be created.

To add a new user group to the server, follow these steps:

1. Start the Full Screen Net Admin Interface and access the server you wish to administer. (For instructions, see the section entitled *Accessing the Full Screen Net Admin Interface*, in Chapter 3).

2. Select the *Accounts* menu and select the *Users/groups* menu item.

The *Users/groups* dialog box appears.

3. Highlight *[NEW]* in the *Groupname* list box (to create a new group).

4. Select the *Add* command button.

   The *Add Group Account* dialog box appears (see Figure 4-4). The default usernames *admin* and *guest* appear in the *Non-members* list box. (Since you are adding a new group, it has no members.)

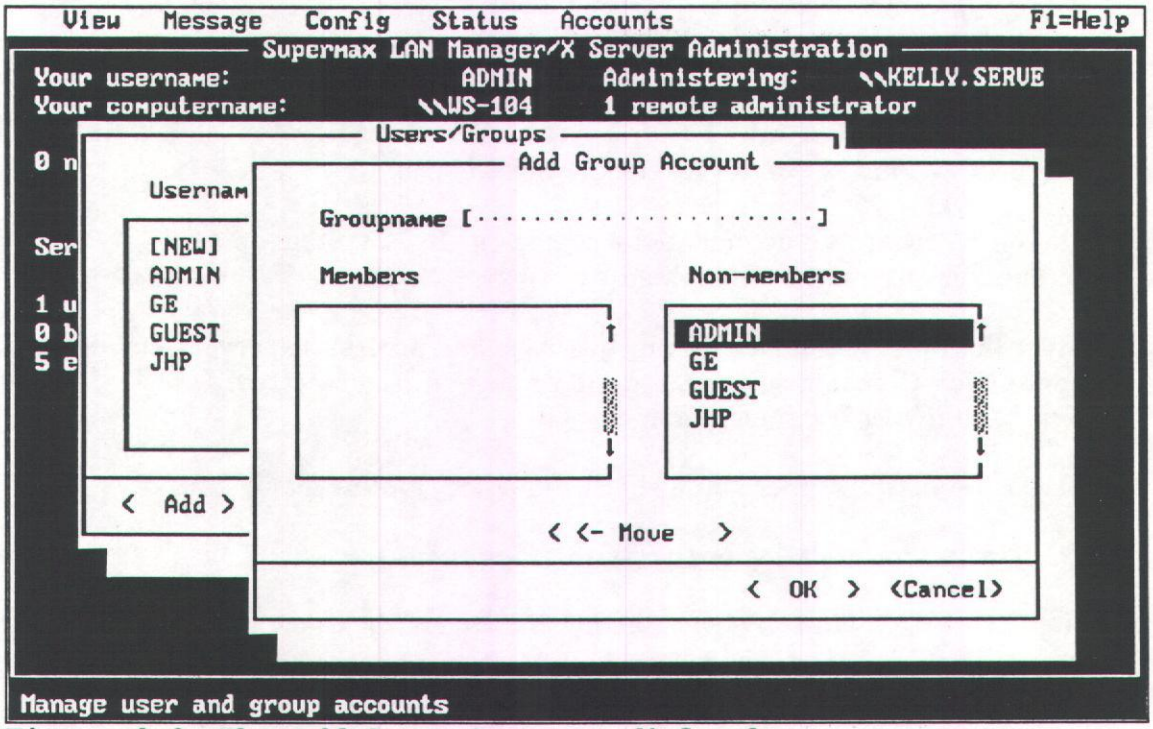


Figure 4-4. The *Add Group Accounts* dialog box

5. At the *Groupname* text box, type the name of the new group.

   The groupname should be easy to remember and reflect the group's purpose. Groupnames can be a maximum of 20 characters long and may be composed of alphanumeric (a-z, A-Z, 0-9) and the following special characters:

   $ % - _ @ { } ~ ' ! # ( ).

   Do not use special national characters. Groupnames are case insensitive.

6. If you want *admin* or *guest* to be a member of this group, use the *Move* command button to move them from the *Not a member of* list box to the *Member of* list box. To do this, highlight the desired username, then select the *Move* command button. Repeat this step as necessary, until the new user group has the desired members.

7. Select the *OK* command button.

8. To add additional groups, repeat Steps 2 through 7 for each group.

After you have completed adding groups, proceed to the next section, *Creating New User Accounts*.

4.4.6.1. Equivalent net Command

You can also add groups to your server using the **net group** command. For more information about the **net group** command, see Chapter 10, *Command Directory*.

4.4.7. Creating New User Accounts

Before performing this procedure, you should have a list of new user accounts to be set up on the server.

To add a user account to the server, follow these steps:

Note: If you also want an account to be used as a UNIX system account, first add the user account through the UNIX system.

1. Start the Full Screen Net Admin Interface and access the server you wish to administer. (For instructions, see the section entitled *Accessing the Full Screen Net Admin Interface*, in Chapter 3.)

2. Select the *Accounts* menu and select the *Users/groups* menu item.

   The *Users/groups* dialog box appears. (Figure 4-5.)

3. Highlight *[NEW]* in the *Username* list box (to create a new user account).

4. Select the *Add* command button.

   The *Add User Account* dialog box appears. (Figure 4-6.)

5. Enter information into the text boxes of the *Add User Account* dialog box as follows:

   a) At the *Username* text box, supply the username for the new user.

      Usernames can be a maximum of 20 characters long and may be composed of alphanumeric (a-z, A-Z, or 0-9) and the following special characters:

      $ % - _ @ { } ~ ‘ ! # ( ).

Usernames are case insensitive.

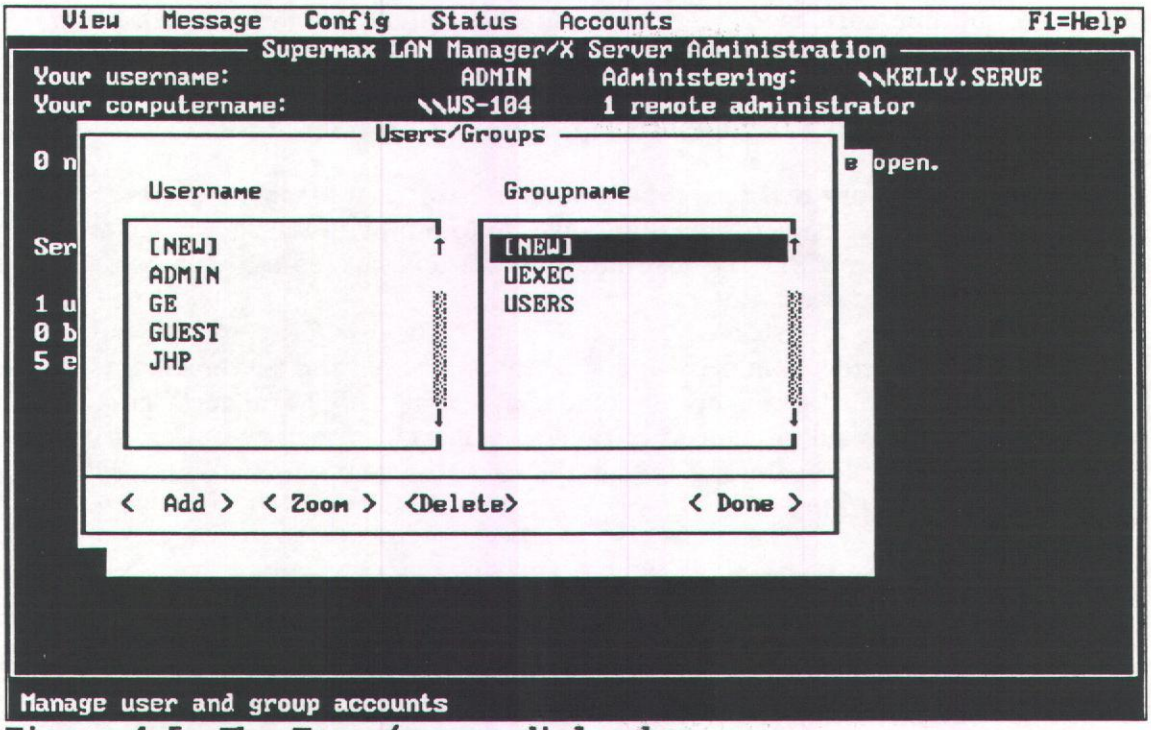


Figure 4-5. The *Users/groups* dialog box

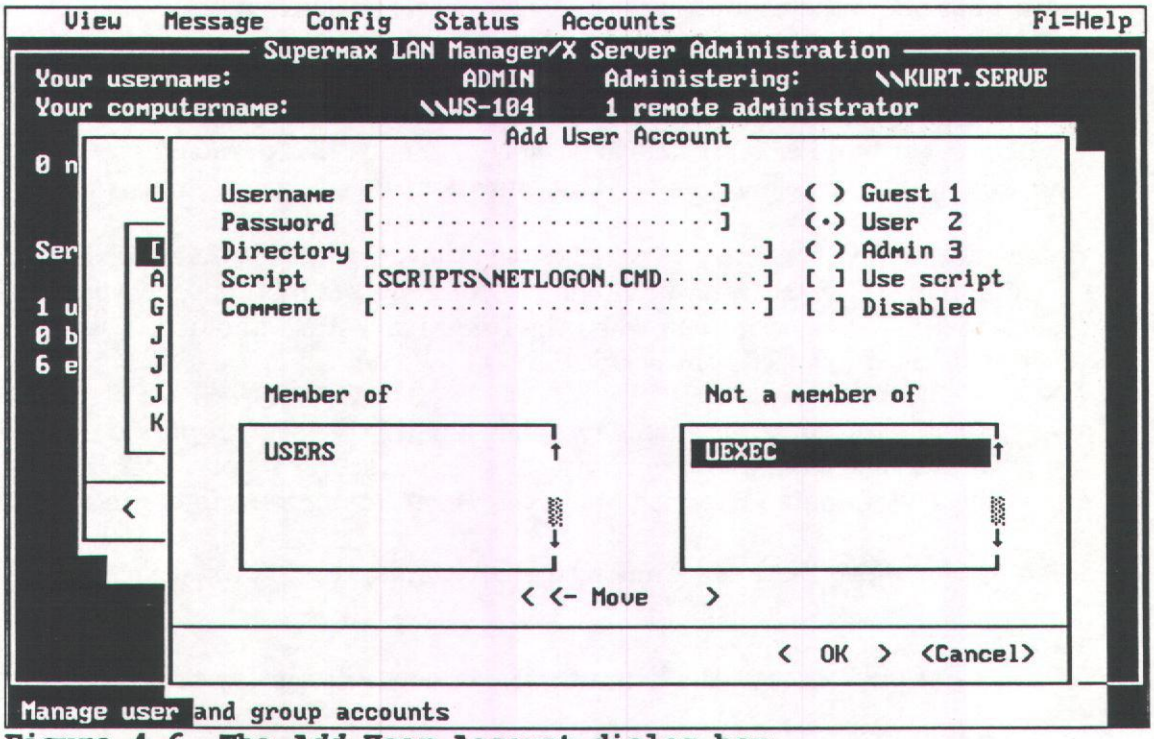


Figure 4-6. The *Add User Account* dialog box

b) At the *Password* text box, assign a password for the user. The allowable characters for a password are the same as those for a username. The maximum allowable length for a password on a server running user-level security is

14 alphanumeric characters. The minimum allowable length for a password is determined by the value of the *minpassword=* parameter in the *[lmxserver]* section of the server's *lanman.ini* file (for more information about this parameter, see Chapter 9, *Changing the Default Server Configuration*).

c) At the *Directory* text box, type a name for the user's home directory on the server. The name you type may have up to 8 alphanumeric characters. Often, administrators enter the username in this text box, so that the home directory name and the username are the same.

A home directory is a private disk storage area on the server for this particular user. Home directories are optional. Supermax LAN Manager/X creates home directories as subdirectories of the */usr/lanman* directory (unless the server has a */usr2* file system; if that is the case, the user's home directory is created in the */usr2/lanman* directory).

Note: If logon validation is disabled, and you want to allow the user to access his or her home directory, you must create a shared directory and grant the user access to this shared directory. The shared directory must be placed in a directory in the path to the user's home directory

If you leave this text box blank, the user will not have a home directory. This will not affect the user's ability to access server resources.

Note: You can specify a different default location for all users' home directories by altering the value of the *userpath=* parameter in the section of the server's *lanman.ini* file. For instructions on how to change this parameter, see Chapter 9, *Changing the Default Server Configuration*.

d) The *Script* text box entry is based on whether or not this server performs logon validation. If this server will validate logon requests by this user, you can optionally have a script run when the logon request is validated. This text box entry is used to specify the script that will be run.

* If you enter only a filename (without a path), the system puts the script file in the */usr/lanman/scripts* directory (if the server has a */usr2* file system, the system puts the script file in the */usr2/lanman/scripts* directory).

  - For Basic DOS and Enhanced DOS clients, the default script is contained in the *netlogon.bat* file.

  - For OS/2 clients, the default script is contained in the *netlogon.cmd* file.

  Caution: If the *Use script* check box is not marked, this server will not perform logon validation for this user, nor will it run the logon script. In addition, this user will not be able to access this server, when the server is configurated to run logon validation.



For more information about logon scripts, see Appendix B, *Managing Logon Validation*.

* If this server is not a logon validator, leave the text box empty. Press the Tab key to move to the next text box. Proceed to Step **e**.

e) At the *Comment* text box, type a descriptive comment identifying this user. This remark can be up to 48 characters long, though the LAN Manager text boxes will not show the entire remark. A typical comment might be the user's full name and phone number. This comment is seen only by administrators of this server.

6. Use the Tab key to move to the column of option buttons on the right of the *Add User Account* dialog box. Select the privilege level for this user (using either the arrow keys or the left mouse button): admin, user, or guest.

7. Mark or unmark the following check boxes as needed:

   Note: To mark a check box, either press the Spacebar once, or, if you are using a mouse, click the left mouse button.

   * `Use script`
     If this server is a logon validator (running logon validation) and you want it to be able to validate this user's logon requests, mark this check box. If this user does not have an account on any other server, and logon validation is being used on the network, you must mark this check box. Otherwise, the user will not be able to log on to the LAN.

     Note: In the case of distributed logon validation, marking the **Use script** check box does not ensure that this server will validate the user. If other servers have a user account for this username and password, any of those servers may perform logon validation for this user.

     If you mark this check box you may also include the pathname of a script in the *Script* text box. The script you specify will run whenever the user successfully logs on to the network.

     For more information about running logon scripts, see Appendix B, *Managing Logon Security*.

   * `Disabled`
     If you want to prevent the user from accessing resources on this server, mark this check box. This is equivalent to temporarily removing this user's account from the server.

8. Use the two list boxes and the *Move* command button to specify the groups to which the user is to belong.

To make the user a member of a group, highlight the desired group in the *Not a member of* list box. Select the *Move* command button.

To remove the user from membership in a group, highlight the group in the *Member of list box*. Select the *Move* command button.

9. Select the *OK* command button.

   * If you did not assign a home directory to the user in Step 5c, the user account is added and you are returned to the background screen. You have completed this procedure. Now you need to grant the new user access to LAN resources. To grant a new user account access to disk resources, see Chapter 7, *Managing Shared Directories*. To grant access to print resources, see Chapter 8, *Managing Shared Printers*.

   * If you assigned a home directory to the user in Step 5c, the system displays the *Edit File Permission* dialog box, allowing you to assign access permissions to the home directory. (Figure 4-7) Using access permissions, you can specify which users or groups can access the directory and the operations they can perform (for example, reading or writing to files in the directory).

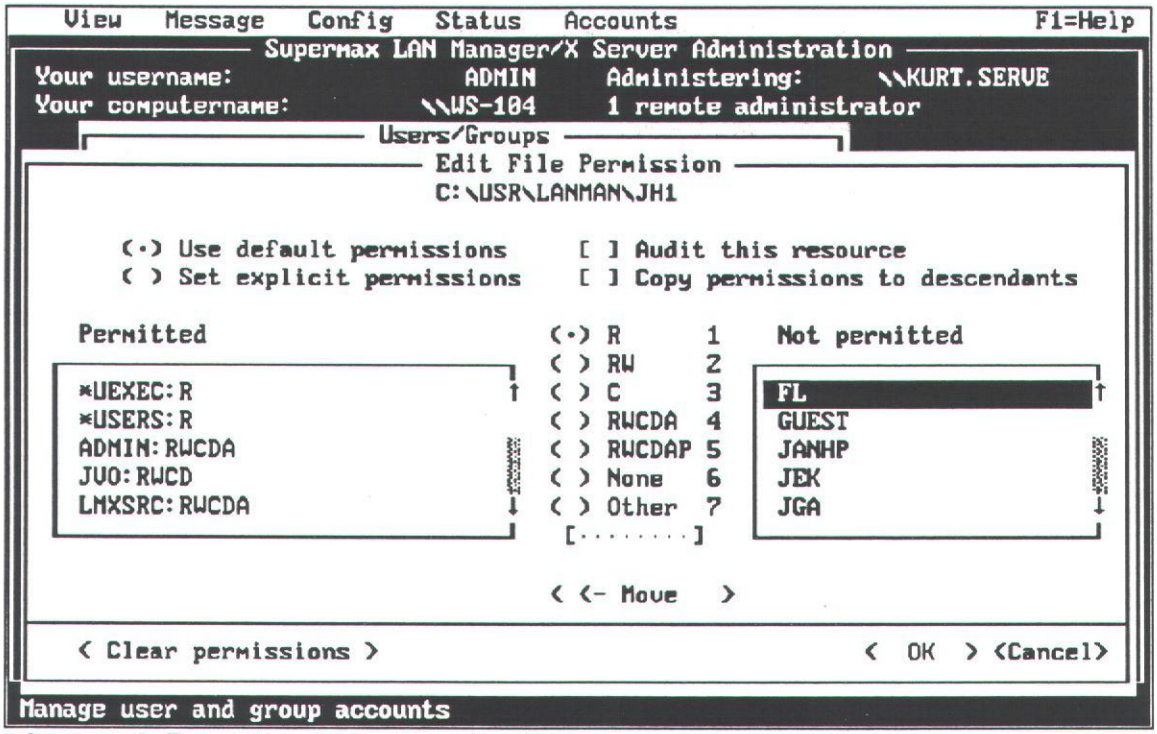


Figure 4-7. *Edit File Permission*

10. Select the *Set explicit permissions* option button.

11. Mark or unmark the following check boxes as needed:



* *Audit this resource*
  If you want to keep track of who uses this home directory, when it is used, and how it is used, mark this check box. To use this feature, the Audit Trail must be enabled on this server (using the *auditing=* parameter in the *[server]* section of the server's *lanman.ini* file). To set the value of this parameter, see Chapter 9, *Changing the Default Server Configuration*.

* *Copy permissions to descendants*
  If you want to assign the same access permissions for this home directory to every directory and file below it in the directory hierarchy, mark this check box.

12. Use the two list boxes, the access permission option buttons, and the *Move* command button to specify which users or groups will be permitted to use this home directory. For each user or group that is permitted to access the directory, you can also specify a unique set of access permissions that control what operations the user or group can perform on the home directory (such as reading or writing to files in the directory). If you wish to limit access to only the owner of the home directory, then make that user the only member of the *Permitted* list box.

    Specify access permissions for each user and group as follows:

    * To add a user or group to the *Permitted* list box, highlight that username or groupname in the *Not permitted* list box. Specify the access permissions you want that user or group to have, using the access permission option buttons. Then select the *Move* command button. The user or group moves to the *Permitted* list box with the access permissions you specified with the access permission option buttons.

    * If you make a mistake and wish to change the access permissions for a user or group that is already in the *Permitted* list box, choose that username or groupname and select one of the access permission option buttons. If you select the *Other* option button, you can type a set of access permissions in the text box below the option button.

      Make sure the new user can access his or her home directory. Access permissions on a new home directory should allow full access (*RWCXDAP*) for the new user and no access (*N*) permission for all others. Remember, giving the user the *P* access permission will allow that user to change access permissions for the home directory.

      Home directories are where users should keep private files on the server. As an administrator, you may need to keep an eye on how much disk space the home directories are consuming and issue warnings accordingly.

13. Select the *OK* command button.

14. To add additional users, repeat Steps 2 through 13 for each user.

You have added a user account to the server. Now you need to grant the new user access to LAN resources. To give a new user account access permissions for disk resources, continue to the next section, *Sharing Directories.*

4.4.7.1. Equivalent net Command

You can also add users using the **net user** command. For more information about the **net user** command, see Chapter 10, *Command Directory*.

4.4.8. Sharing Directories

When you share a directory, you make all files and subdirectories of that directory available to specified users on the LAN.

Before performing this procedure, you should have a list of all directories you need to share on the server. You also need a list of users and groups that will be permitted to access each shared directory. For more information about determining which directories should be shared and the access permissions that should be assigned to them, see the section earlier in this chapter entitled, *Planning the Server Configuration.*

To share a directory on your server, follow these steps:

1. Start the Full Screen Net Admin Interface and access the server you wish to administer. (For instructions, see the section entitled *Accessing the Full Screen Net Admin Interface*, in Chapter 3, *Using the Administrative Interfaces.*)

2. Select the *View* menu and select the *This server* menu item.

   The *Resources This Server is Sharing With the Network* dialog box appears. This dialog box displays all resources currently being shared from the server (at this point in the set up process, the only shared resources to appear should be the default shared directories and any home directories you have created).

3. Select the *Add share* command button.
   The *What would you like to share?* dialog box appears.

4. Select the *Disk directory* option button.

   The *Share a Disk Resource With the Network* dialog box appears.

5. Enter information into the text boxes of the *Share a Disk Resource With the Network* dialog box as follows:

   a) At the *Sharename* text box, type the sharename for the directory being shared. This is the shared resource name that users will link to when they need to access the directory's contents.

      Sharenames for directories can be a maximum of 8 alphanumeric characters.

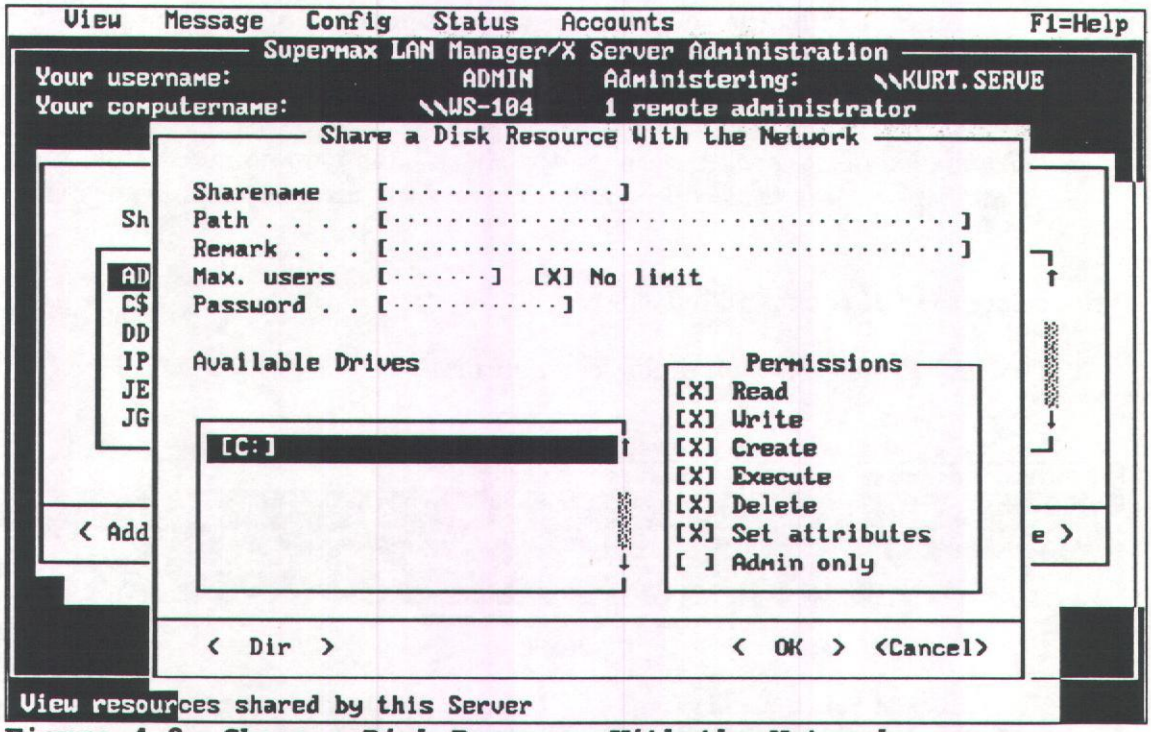


Figure 4-8. *Share a Disk Resource With the Network*

b. At the *Path* text box, type the drive letter and path of the server directory you are sharing.

The format of the path statement is as follows:

```
driveid:\directory\subdirectory
```

Where *driveid* is the drive (usually C: for the server's hard disk) where the shared directory is stored; and *\directory\subdirectory* is the UNIX system pathname for the shared directory (note the use of backslashes between directory names).

If you specify a path that contains a directory that does not exist, LAN Manager will attempt to create that directory. In such cases, you should specify a path that starts with the default administerable LAN Manager directories (such as the *c:\usr\lanman* or *c:\usr\lanman2* directories). For more information about specifying the proper path, refer to the section entitled *Recommended Locations for Creating New Shared Directories*, earlier in this chapter.

c. At the *Remark* text box, type a comment describing the directory.

d. Do *one* of the following:

* At the *Max. users* text box, type the maximum number of users that will be able to access the directory simultaneously. For example, this number may

be determined by the software license agreement of a network application program that will be stored in the directory. Such license agreements can specify the maximum allowable number of simultaneous users.

* At the *No limit* check box, mark the check box if you do not wish to limit the number of users that will be able to access the directory simultaneously.

e. Select the *OK* command button.

The *Edit File Permission* dialog box appears.

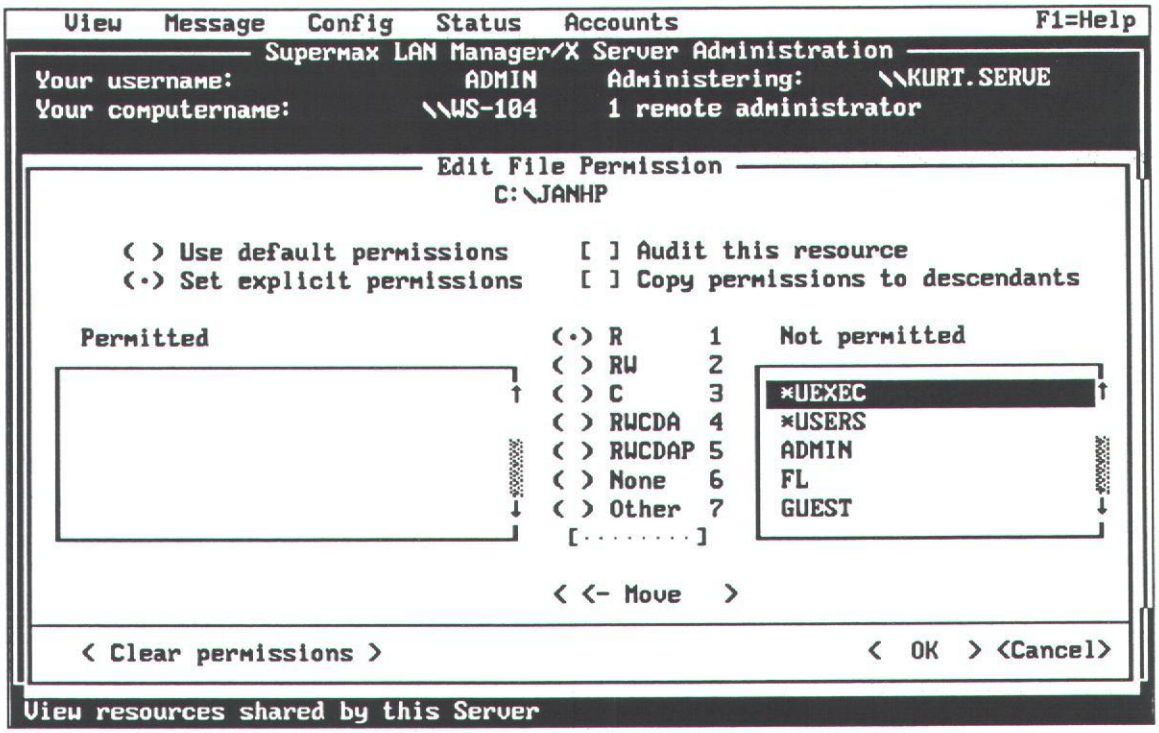


Figure 4-7. *Edit File Permission*

6. Specify which users and groups can access the new shared directory and what kind of access permissions they will have. For each user or group that is permitted to access the shared directory, you can specify a unique set of access permissions that control what operations the user or group can perform on the shared directory (such as reading or writing to files in the directory). If you wish to limit access to only one user, then make that user the only member of the *Permitted* list box.

Assign access permissions for the new shared directory as follows:

* Determine whether or not you wish to assign the system's default access permissions to the users and groups that will access the shared directory:



* If you wish to assign the system default access permissions to users and groups that will access the shared directory, select the *Use default* permissions option button.

  Note: You will not be able to use default access permissions if the new shared directory is a subdirectory of other shared directories that are configured for explicit access permissions.

* If you wish to assign access permissions manually for the users and groups that will access the shared directory, select the *Set explicit permissions* option button.

  There are two ways to assign explicit access permissions:

  - To assign the same access permissions to many users and groups, first specify the desired access permission by selecting the proper option button. Then move the users and groups from the *Not permitted* list to the *Permitted* list by highlighting the user or group and selecting the *Move* command button.

  - To assign different access permissions to various users and groups, first move the users and groups from the *Not permitted* list to the *Permitted* list by highlighting the user or group and selecting the *move* command button. Then assign access permissions individually, by highlighting the user or group in the *Permitted* list and then assigning the desired access permission by selecting the proper option button.

* Mark the *Audit this resource* check box if you want to record who uses this shared directory, when it is used, and how it is used. To use this feature, the Audit Trail must be enabled on this server (using the *auditing=* parameter in the *[server]* section of the server's *lanman.ini* file). To set the value of this parameter, see Chapter 9, *Changing the Default Server Configuration*.

* Mark the *Copy permissions to descendants* check box if you want to assign the same access permissions that apply to this directory to every directory and file below it in the directory hierarchy.

7. Select the *OK* command button.

   The system closes the *Edit File Permission* dialog box. The *Resources This Server Is Sharing With the Network* dialog box appears. The sharename for the shared directory you just created should appear in the display.

8. Determine whether or not you want to share additional directories:

   * To share additional directories, repeat Steps 2 through 7 for each directory you want to share.

   * To close the *Resources This Server Is Sharing With the Network* dialog box, select the *Done* command button.

When you have completed sharing directories, continue to the next section, *Setting Up Shared Print Queues*.

4.4.8.1. Equivalent net Command

You can also share directories using the **net share** and **net access** commands. For more information about these commands, see Chapter 10, *Command Directory*.

4.4.9. Setting Up Shared Print Queues

This section contains procedures for configuring and sharing printers that are *physically connected to the server*. For complete information about sharing printers, and for instructions about creating customized print processor scripts, see Chapter 8, *Managing Shared Printers*.

4.4.9.1. Configuring Printers

After you have connected the printer to your server, you must set up the printer port (to connect and configure the printer itself, see the instructions included with the printer). To configure the printer port on the UNIX system, see Chapter 7, *Lp Spooler Administration* in the *Supermax System V, System Administrator's Guide*.

Confirm that the printer is set up correctly by following these steps:

1. **a)** Log on as *root* at the console, if you have not done so already. At the UNIX prompt, type:

   ```
   lp -d printername  /etc/passwd
   ```

   where *printername* is the name of the printer you want to check. Press RETURN.

   b) Review the results of the test and respond accordingly:

   * If the printer prints out the */etc/passwd* file (a list of UNIX system logins on your server), then it is functioning properly as a UNIX system printer.

   * If the printer does not print out the */etc/passwd* file, a problem has occurred. First make sure that the printer is plugged in and powered on. Then check the printer cable installation. Finally, check the printer configuration information. Then repeat step 1.

   For additional troubleshooting information, see Chapter 7 in the *Supermax System V, System Administratior's Guide*.

When you have completed configuring the UNIX system for this printer, the printer can be used by users logged in to the server's UNIX system. However, to allow LAN Manager network users to access this printer, you must now create a shared print queue. For more information, see the next section, *Sharing Print Queues*.

4.4.9.2. Sharing Print Queues

To share a printer that is connected to the server, follow these steps:

1. Start the Full Screen Net Admin Interface and access the server on which you want to share a printer. (For instructions, see the section entitled *Accessing the Full Screen Net Admin Interface*, in Chapter 3).

2. Select the *View* menu and select the *This server* menu item.

   The *Resources This Server Is Sharing With the Network* dialog box appears.

3. Select the *Add share* command button.

   The *What would you like to share?* dialog box appears.

4. Select the *Spooled printer* option button and then select the *OK* command button.

   The Share a Print Queue With the Network dialog box appears. (Figure 4-8).

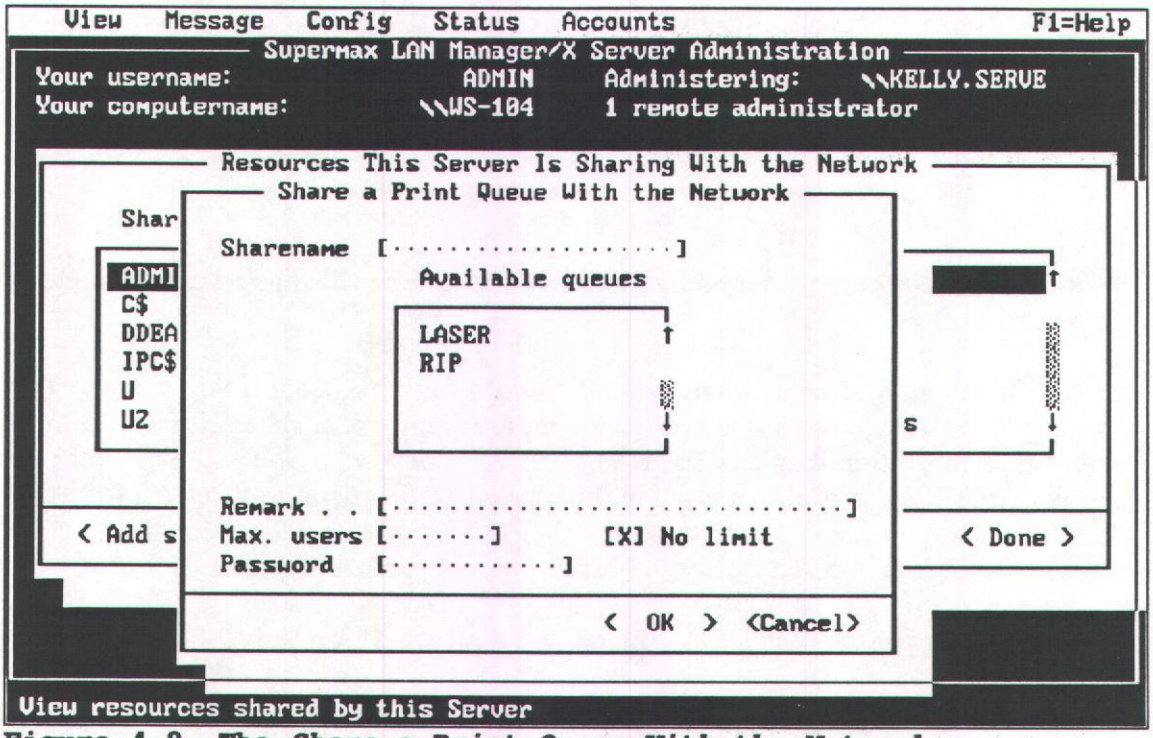


Figure 4-8. The *Share a Print Queue With the Network*

5. Enter information into the text boxes of the *Share Print Queue With the Network* dialog box as follows:

   a) At the *Sharename* text box, type the sharename you want the shared print queue to have. Do not enter a name that is already being used by any of the

server's UNIX system *lp* devicenames (printer names). If you share multiple print queues on the server, each of their sharenames must be unique.

Sharenames for shared print queues can have up to 8 alphanumeric characters.

b) At the *Remark* text box, type a comment describing the shared print queue.

c) At the *Max. users* text box, type the maximum number of users that will be able to use this queue at any one time. If you do not wish to set a maximum number of users, mark the *No limit* check box.

d) The *Password* text box is not used on servers running user-level security. On servers running share-level security, at the *Password* text box, enter a password for the shared print queue to prevent unauthorized use. On servers running share-level security, up to 8 alphanumeric characters may be used. The minimum allowable length for a password is determined by the value of the *minpassword=* parameter in the *[lmxserver]* section of the server's *lanman.ini* file (for more information about this parameter, see Chapter 9, *Changing the Default Server Configuration*).

6. Select the *OK* command button.

Since the shared print queue does not already exist, a message box displays this message:

```
The specified printer queue does not exist.
Click <OK> to create the queue <sharename>.
```

where *<sharename>* is the name you have chosen for the shared print queue. Proceed to Step 7.

Note: If the shared print queue already exists (only possible if you are sharing multiple printers), the system displays an error message. Select the *OK* command button. The system displays the *Resources This Server Is Sharing With the Network* dialog box. Choose a new name for the shared print queue and return to Step 3.

7. Select the *OK* command button to create the shared print queue.

The *Printing Options for Queue* dialog box appears. (Figure 4-9).

8. Enter information into the text boxes of this dialog box as follows:

a) At the *Priority* text box, set the priority for this queue by typing a number between 1 and 9. (1 is the highest priority, 9 is the lowest, and 5 is the default setting.)

b) At the *Printer device(s)* text box, type the UNIX system *lp* printer names

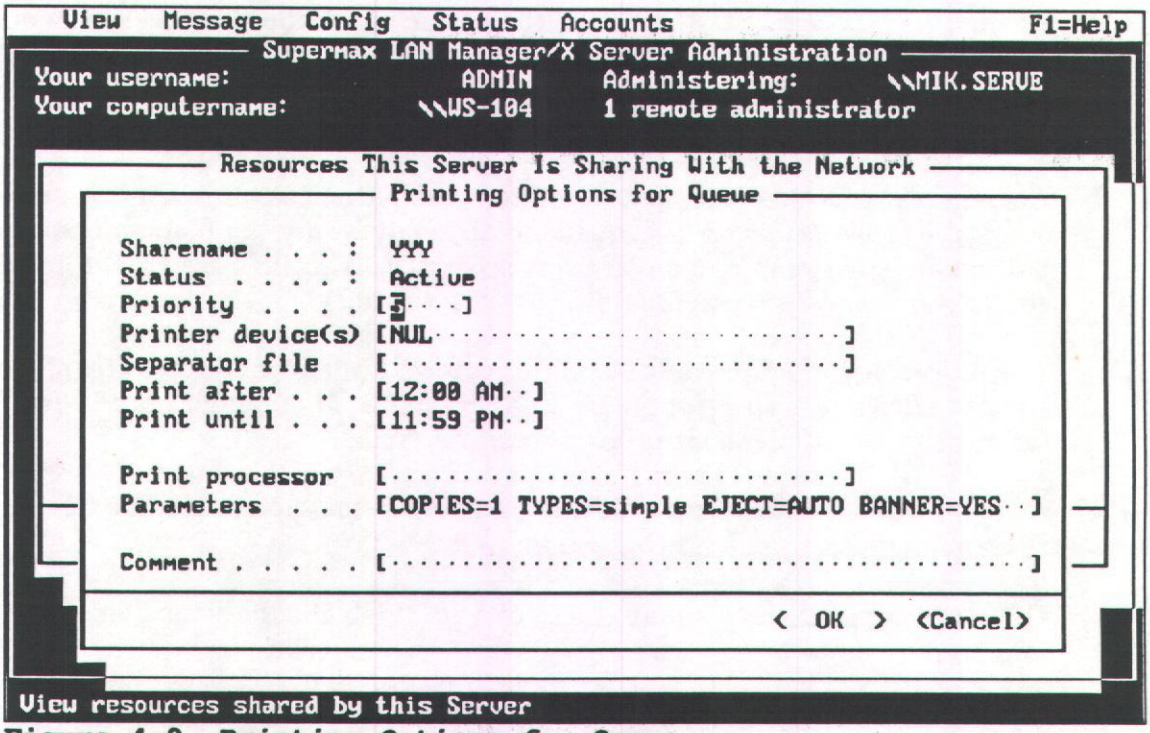


Figure 4-9. *Printing Options for Queue*

(printer names, as defined in the previous procedure, entitled *Configuring Printers*) for the printer(s) to be included in the queue. The physical printers specified here will be the printers that actually print jobs submitted to this shared print queue.

If the shared print queue will route print jobs to a pool of printers, separate the *lp* printer names with spaces. For example,

```
laser1 laser2
```

Leave this text box set to *NUL* if this queue will use a print processor script.

c) At the *Separator file* text box, type the pathname of the separator file you want to use with this queue, if any. This can be a relative pathname or an absolute pathname. Relative pathnames are assumed to begin in the */usr/net/servers/-lanman/spool* directory; absolute pathnames are assumed to begin at the server's root (/) directory. If you want to use the default banner page, leave this field blank.

d) At the *Print after* text box, type the time at which the shared print queue can start sending requests to the printer(s). Use *either* 24-hour format (00:00 -23:59) or 12-hour format (12:00 AM - 11:59 PM). The printer will begin printing within ten minutes of the time you specify.

e) At the *Print until* text box, type the time after which the shared print queue can no longer send requests to the printer(s). Use *either* 24-hour format (00:00 - 23:59) or 12-hour format (12:00 AM - 11:59 PM). The printer will stop printing within ten minutes of the time you specify.

f) At the *Print processor* text box, type the name of the customized print processor script file to be used with this queue, if any. Enter only the filename (a full pathname is not required, as all print processor script files are stored in the server's */usr/net/servers/lanman/customs* directory).

A print processor script can be used to perform customized processing of jobs submitted to a shared print queue. See Chapter 8, *Managing Shared Printers*, for more information about print processor scripts.

g) At the *Parameters* text box, type any parameters for the queue. The Server Program supports the following parameters:

COPIES - specifies how many copies of a print job should be printed. Specify a number.

TYPES - specifies the content type (also known as the file type) of the files that will be sent to the queue by default. The content type accepted by a queue is determined by the content type accepted by the first printer specified in the queue. Therefore, once you complete the *Printer Device(s)* text box and press RETURN, the *TYPES* field will automatically contain the content type for the first printer specified in the text box.

Note: Normally, you will not need to change the value in the *TYPES* field from the value that automatically is assigned to it. However, if you are sending ASCII files to a printer queue which contains PostScript printers, the *TYPES* field should be set to *simple*. If you do not set this field to *simple*, the job will not print (although you will receive a message that the job has printed). For more information about content types, see the section on configuring printers in the *Supermax System V, System Administrator's Guide*.

EJECT - specifies whether or not a page feed should occur between copies for multiple-copy print jobs. Specify `auto` (default) or `yes` if you want page feeds between copies. Otherwise, specify `no`.

BANNER - specifies whether or not to print a separator page (banner) between print jobs. Specify `yes` or `no`.

h) At the *Comment* text box, type a comment describing the shared print queue.

9. Select the *OK* command button.

The *Add Permissions* dialog box appears.

10. Determine how you want to specify access permissions for the queue:

    * If you want to use the default access permissions, select the *Use default permissions* option button. This will assign the *Yes* access permission to the default set of users and groups (configured with the *PRINT* special printer resource). Proceed to Step 11.

    * If you want to specify access permissions for the queue on an individual user and group basis, select the *Set explicit permissions* option button.

      Use the two list boxes, the access permission option buttons, and the *Move* command button to specify the access permissions for each user and group as follows:

      - To add a user or group to the *Permitted* list box, highlight that username or groupname in the *Not permitted* list box, select the *Yes* access permission option button, and select the *Move* command button. The user or group moves to the *Permitted* list box, with the *Yes* access permission assigned. Each resource can have up to 64 entries in the *Permitted* list box.

        Note: If the access permission option button is set to *No* when you move a username into the *Permitted* list box, then you are preventing that user from using the resource. This occurs regardless of the groups to which that user belongs.

      - To remove a user or group from the *Permitted* list box, highlight that username or groupname and select the *Move* command button.

      - To change the access permissions for a user or group in the *Permissions* list box, highlight that username or groupname and select one of the access permission option buttons.

11. If you want to record who uses this queue, when it is used, and what is done with the queue, mark the *Audit this resource* check box. To use this feature, the Audit Trail must be enabled on this server (using the *auditing=* parameter in the *[server]* section of the server's *lanman.ini* file). To set the value of this parameter, see Chapter 9, *Changing the Default Server Configuration*. For more information on resource auditing, see the *Supermax LAN Manager/X Troubleshooting and Command Reference*.

12. Select the *OK* command button.



4.4.9.3. Equivalent net Command

You can also create a shared print queue using the **net share** command. After creating the shared print queue, you can reconfigure its options using the **net print** command. For more information about the **net share** and the **net print** commands, see Chapter 10, *Command Directory*.

You have now completed configuring and sharing printers connected to your server. For more information on sharing printers and creating customized print processor scripts, see Chapter 8, *Managing Shared Printers*.

You have now set up your server in its default configuration. You may either accept this default configuration or modify your server configuration to more closely match the needs of your LAN users.

To change the server's default configuration, see Chapter 9, *Changing the Default Server Configuration*.

To accept the default configuration and learn about managing day-to-day server operations, see Chapter 5, *Managing Server Operations*.

5. Managing Server Operations

5.1. Overview

This chapter contains procedures and information needed to manage the day-to-day operations of the server, including instructions for performing the following tasks:

* Stopping and restarting the server
* Displaying the Audit Trail
* Listing servers and resources available on the LAN
* Clearing or changing an administrative password
* Running the command-line administration utility

Each of these tasks is described in the sections which follow.

5.2. Stopping and Restarting the Server

You can stop and restart the operation of the Server Program from a terminal connected to the server. This section contains procedures for performing these tasks.

5.2.1. Stopping the Server Program

Stopping the Server Program prevents users from accessing server resources.

Before stopping the Server Program, you should send a message advising users that the server is coming down. To do this, follow these steps:

1. Start the Full Screen Net Admin Interface and access the server you wish to administer. (For instructions, see the section entitled *Accessing the Full Screen Net Admin Interface*, in Chapter 3.)

2. Select the *Message* and select the *Send* menu item.

   The *Send a message* dialog box appears.

3. Select the *All users of this server* option button.

4. Type your message in the *Message text* text box. Press RETURN to send the message.

   The message should indicate that the server will be stopped, and it should advise users to complete their work and disconnect their links to the server immediately. Provide users with adequate time to close their files before you proceed.If the server is stopped while users are accessing its shared resources, data may be lost.

5. Exit the Full Screen Net Admin Interface. (For instructions, see the section entitled *Exiting the Full Screen Net Admin Interface*, in Chapter 3.)

   Wait until all users have stopped accessing the server. You can use the **net session** command to list sessions and assoicated username between the server and other computers on the local area network. To stop the Server Program immediately, you should log on as the UNIX system administrator *root* from a terminal and type

   ```
   /usr/bin/lmx/lmxmgmt stop
   ```

5.2.2. Restarting the Server Program

Restarting the server does not require that you reboot the computer. Just log on as the UNIX system administrator *root* or *lmxadmin* from a terminal and type

```
/usr/bin/lmx/lmxmgmt start
```

The command

```
/usr/bin/lmx/lmxgmt restart
```

can be used to stop and immediately start the server.

Note: After the Server Program is restarted, clients may automatically re-establish links that existed to the server before the Server Program was stopped.

5.3. Displaying the Audit Trail

For each resource being audited, the Audit Trail records when the resource was accessed, who accessed it, and what was done with it.

Note: The Audit Trail is only available on servers running user-level security.

The Audit Trail records only the opening of connections, not subsequent actions that involve the resource. For example, individual reads to a file are not recorded, only the initial open.

To display the contents of the Audit Trail, follow these steps:

1. Start the Full Screen Net Admin Interface and access the server you wish to administer. (For instructions, see the section entitled *Accessing the Full Screen Net Admin Interface*, in Chapter 3.)

2. Select the *Status* menu and select the *Audit trail* menu item.

   The *Network Audit Trail* dialog box appears. (Figure 5-1).

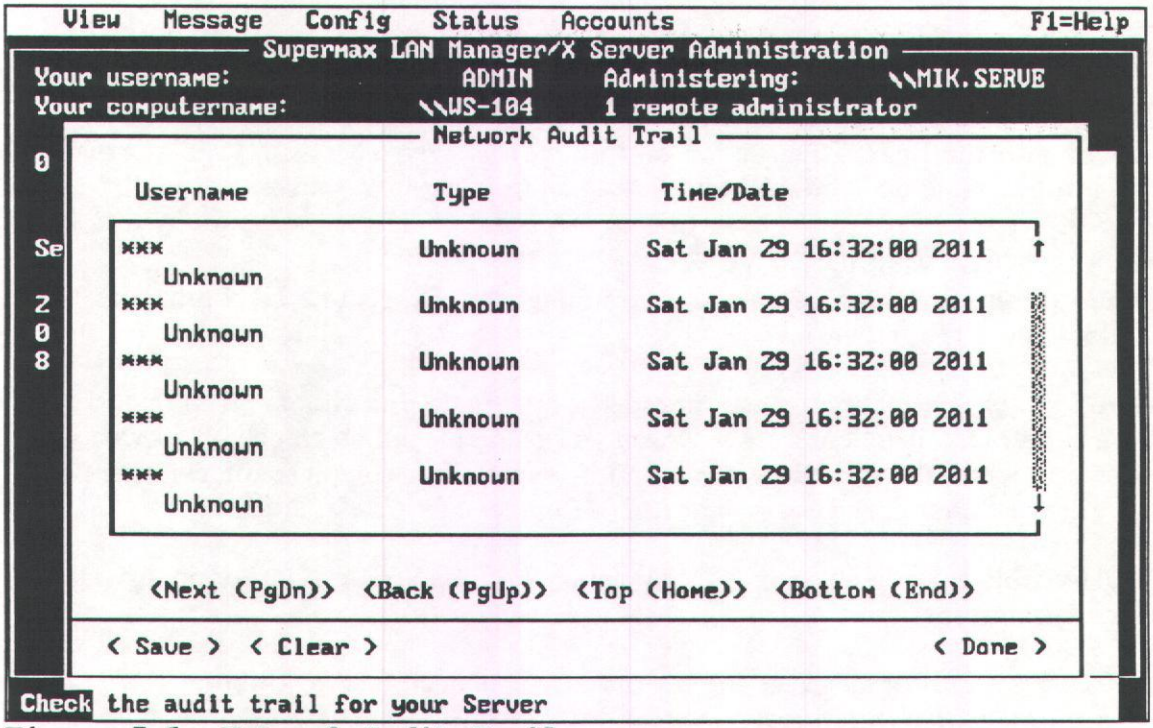


Figure 5-1. *Network Audit Trail*

This dialog box displays attempts (successful and unsuccessful) by users to access server resources. Specifically, it shows the

* username of the person who requested access
* the type of access requested. There are several such types:

Type of access	Context
Server	for server actions
Session	for user sessions
Share	for starting and stopping sharing
Access	for access by users
Access denied	for access violations
Other	for other actions

* the time and date of the operation
* a brief description of what operation was performed or attempted

5.4. Listing Servers and Resources Available on the LAN

The Server Program allows you to see the names of the other servers that are available for use on the LAN. It also lets you list the resources that are being shared by those servers with the LAN. This section contains procedures for listing visible servers (those that are available on the LAN) and listing shared server resources.

5.4.1. Listing Visible Servers

Visible servers are those servers that are members of the same LAN group and are available over the network.

A *LAN group* is a distinct group, or subset, of servers and clients on the network. Only those servers in the client's LAN Group will be displayed on the client in various dialog boxes and when the **net view** command is issued. (For complete information about the **net view** command, see *Supermax LAN Manager/X - User's Guide*.)

To list visible servers on your LAN by using the Full Screen Net Admin Interface, follow these steps:

1. Start the Full Screen Net Admin Interface, as described in Chapter 3, *Using the Administrative Interfaces*.

2. Select the *View* menu and select the *Network servers* menu item.

   The *Servers Available on Network* dialog box appears, listing the visible servers on your network.

   Note: A server can be hidden from such a display if the *srvhidden=* parameter in its *lanman.ini* file is set to *yes*.

If a server listed is sharing resources, you can use the shared resource by redirecting a local device to the remote resource.

Note: You cannot redirect local devices while administering a remote server.

5.4.2. Listing Shared Server Resources

When you want to share a new resource from your server, you should first determine which resources you are currently sharing and identify their corresponding sharenames. You can list the server's shared resources using either the Full Screen Net Admin Interface or the Command Line Net Interface.

To list shared resources for a server using the Full Screen Net Admin Interface, follow these steps:

1. Start the Full Screen Net Admin Interface and access the server you wish to administer as described in Chapter 3, *Using the Administrative Interfaces*.

2. Select the *View* menu and select the *This server* menu item.

   The *Resources This Server Is Sharing With the Network* dialog box appears. (Figure 5-2).

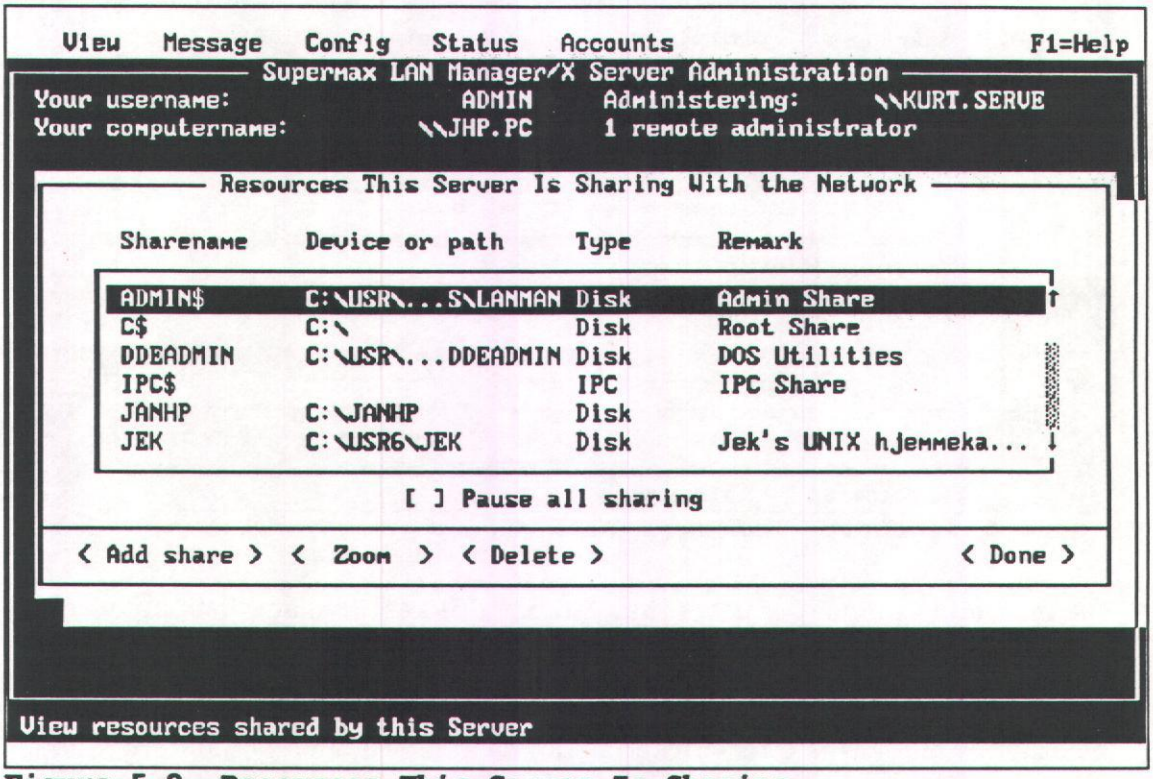


Figure 5-2. *Resources This Server Is Sharing ...*

The list box in this dialog box shows the sharename, the path or devicename, the resource type, and a remark for each shared resource.

There are three kinds of resources that can appear in this list box:

* The reserved administrative resources *IPC$* and *ADMIN$*

* The reserved sharenames for the server's hard disk drives (such as *C$*).

* Any resources that are shared on this server.

3. To see more information about a shared resource, select that resource from the list box and select the *Zoom* command button.

   The *Shared Resource Information* dialog box appears. (Figure 5-3).

   This dialog box repeats all of the information for this resource that was available in the *Resources This Server Is Sharing With the Network* dialog box. It also shows

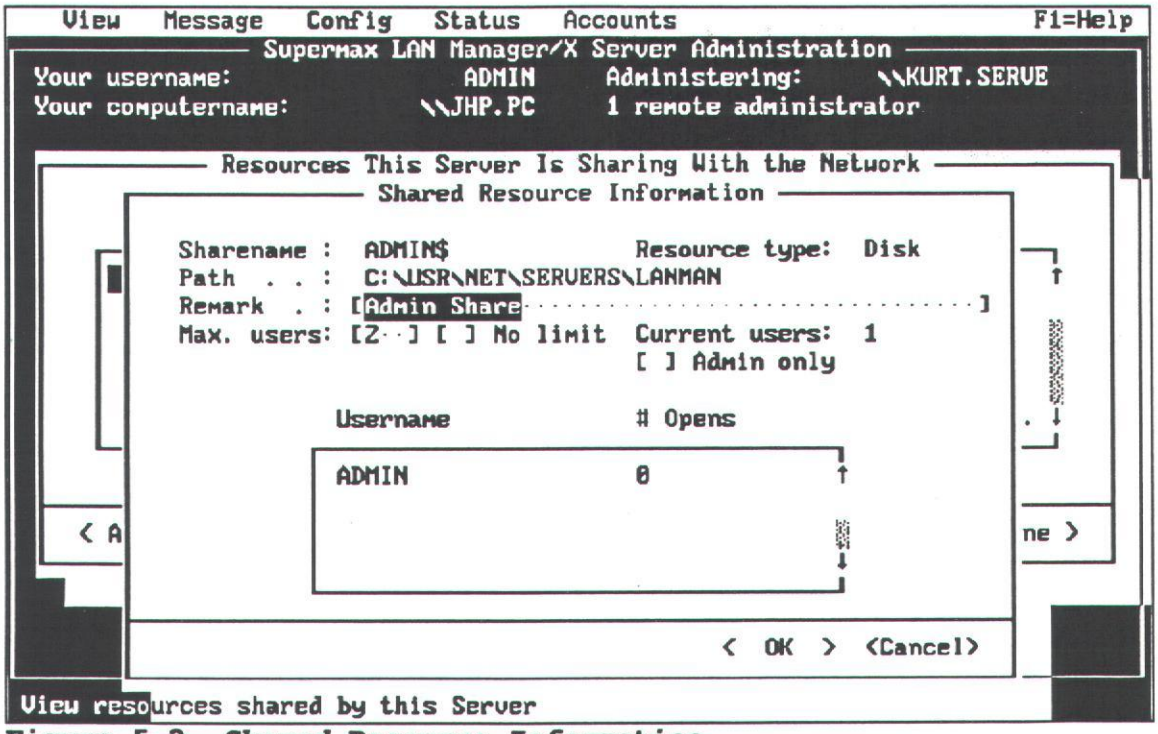


Figure 5-3. *Shared Resource Information*

the maximum number of users that can use this resource and lists all users who are currently using the resource.

If your server is running user-level security, the *Admin only* check box shows whether or not this is a resource that can be accessed only by administrators. For share-level servers, this dialog box shows access permissions for this resource and contains a text box that you can use to change the resource's password.

Example

You are the administrator for the *mis.serve* server, and you are preparing to share a new resource. Before sharing the resource, you want to see how the server is currently set up. In particular, you want to find out which users are currently using shared resources on the *mis.serve* server.

Using the Full Screen Net Admin Interface, you access the *mis.serve* server.

From the *View* menu, you select the *This server* menu item. In the list box of the *Resources This Server Is Sharing With the Network* dialog box, you see only one printer queue. You select it, and then select the *Zoom* command button. In the *Shared Resource Information* dialog box, you see that eight users are currently using the printer queue, and that eight is also the maximum number of users that are allowed to use the resource at one time. It is time to share a new printer from this server.

5.4.3. Equivalent net Command

You can also list the server's shared resources using the **net share** command. For more information about the **net share** command, see the Chapter 10, *Command Directory*.

5.5. Clearing or Changing an Administrative Password

When the Server Program is installed, an administrative login (*admin*) is created automatically. This enables you to log in as the administrator and perform server management tasks such as adding users, sharing directories and printers, and managing printer queues.

The Server Program creates the *admin* login and prompts you for a password when the software is installed. To protect the login from unauthorized use you can use the Full Screen Net Admin Interface to clear or change that password.

To clear or change the *admin* password by using the Full Screen Net Admin Interface, follow these steps:

1. Start the Full Screen Net Admin Interface and access the server you wish to administer, as described in Chapter 3, *Using the Administrative Interfaces*.

2. Select the *Config* menu and then the *Change password* menu item.

   The *Change Logon Password at a Server* dialog box appears. (Figure 5-4).

3. Enter the old password in the *old password* text box.

   Note: The maximum available length for a password on a server running user-level security is 14 alphanumeric characters (on servers running share-level security, up to 8 alphanumeric characters may be used). The minimum allowable length for a password is determined by the value of the *minpassword=* parameter in the *[lmxserver]* section of the server's *lanman.ini* file (for more information about this parameter, see Chapter 9, *Changing the Default Server Configuration*).

   * To change the password, enter a new password in the *new password* text box.

   * To clear the password, do not enter anything in the *new password* text box.

4. Select the *OK* command button.

   The system closes the *Change Logon Password at a Server* dialog box and a message appears showing the result of your command.

   Press RETURN when the message has been read.

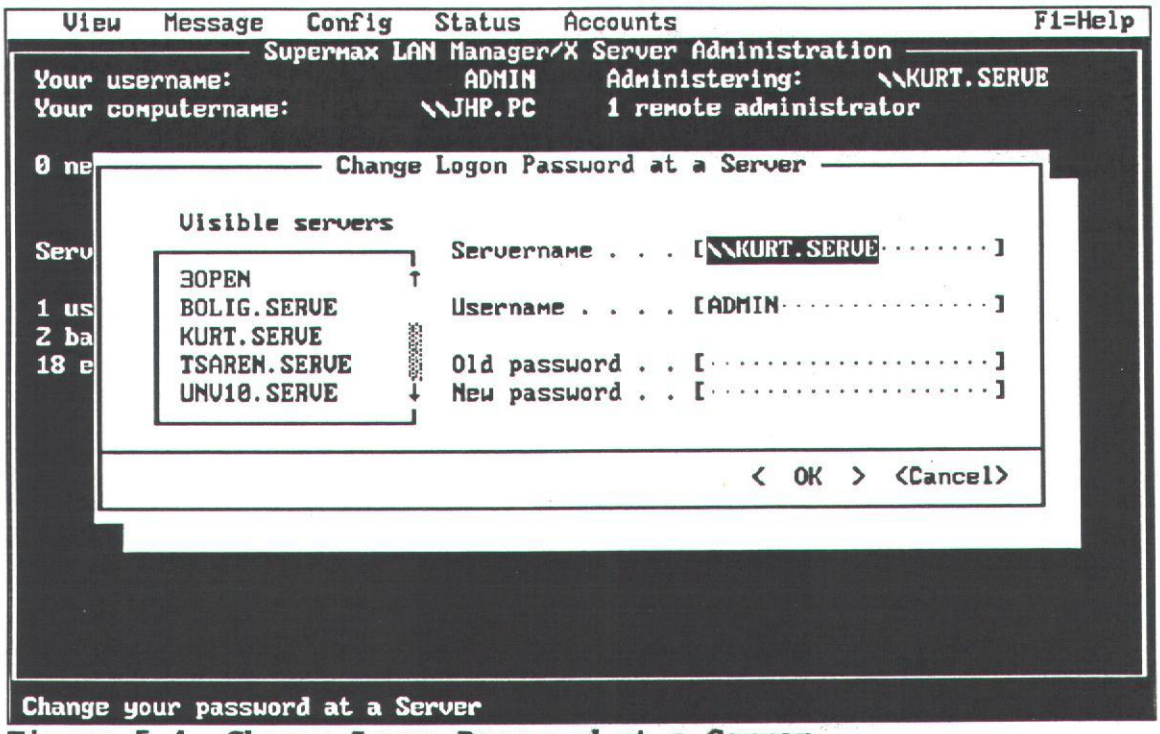


Figure 5-4. *Change Logon Password at a Server*

5.5.1. Equivalent net Command

You can also change the *admin* password using the **net password** command. For more information about the **net password** command, see Chapter 10, *Command Directory*.

5.6. Running the Command-Line Administration Utility

From a terminal connected to your server you can run a command-line administration utility to administer LAN Manager servers.

Only one user with system administration privileges should be using this command at any given time. Otherwise, data could be lost.

To run the command-line administration utility follow these steps:

1. Log on as the UNIX system user *lmxadmin* or *root* from a terminal on the server or via a terminal emulator.

2. Run the */usr/bin/lmx\lineadm* program.

   The *Running the Command Line Administration Utility* form appears.

3. In the *Servername* field, enter the name of the server you want to administer and press RETURN. The correct format is `sname`**`.serve`** where *sname* is the servername of the server you want to administer.

4. In the *Username* field, enter the proper name, depending upon the type of server you want to administer. Press RETURN.

   * If the server you want to administer is running user-level security, enter the administrative username (*admin*).

   * If the server you want to administer is running share-level security, enter any valid username.

5. In the *Password* field, enter the appropriate password, depending upon the type of server you wish to administer. Press RETURN.

   * If the server you want to administer is running user-level security, enter the password for the username you entered in step 3.

   * If the server you want to administer is running share-level security, enter the password for the *ADMIN$* directory.

     Note: If the *ADMIN$* directory does not have a password, any valid username can be used to administer the server.

   The Command Line Net Interface will appear with the *sname.serve* prompt to the left of the command line (*sname* is replaced with the servername of the server you have specified).

6. When you want to exit the the command-line administration utility, type **`exit`** and press RETURN.

6. Managing Users and Groups Under User-Level Security

6.1. Overview

After setting up a server running user-level security, your role as administrator is largely one of maintenance. You maintain the user accounts and groups, adding or deleting them as necessary. You also assign access permissions each time you share a new resource. You can modify existing accounts and access permissions at any time, to meet the needs of the LAN.

This chapter describes how to

* Add user accounts
* Remove user accounts
* Change user passwords
* Display existing user accounts
* Add user groups
* Remove user groups
* Administer the uexec group

Each of these tasks is described in the following sections.

6.2. Managing Users

A *user* is anyone who uses a server's resources. A user who wants to access resources on a user-level server must either have a user account on that server, or must be able to access the guest user account.

This section contains procedures for performing the following user management tasks:

* Adding user accounts
* Changing user passwords
* Removing user accounts
* Displaying existing user accounts

6.2.1. Adding User Accounts

You need to add user accounts to a server when:

* You are installing a server.

* You add a new client to the LAN. If the person or people who are to use the client already have accounts on this server, you do not need to add any new accounts.

* A new person needs to use the server's resources.

* You want to establish an anonymous account. Sometimes you may want to create an account not tied to any particular person, such as a guestprtr account for people who only need to use the server for occasional printing. It is usually more efficient to establish groups for this purpose; anonymous accounts are a potential security problem.

Note: If you also want an account to be used as a UNIX system account, first add the user account through the UNIX system.

To add a user account to the server, follow these steps:

1. Start the Full Screen Net Admin Interface and access the server you wish to administer. (For instructions, see the section entitled *Accessing the Full Screen Net Admin Interface*, in Chapter 3.)

2. Select the Accounts menu and select the *Users/Groups* menu item.

   The *Users/Groups* dialog box appears. (Figure 6-1).

3. Highlight the appropriate item in the *Username* list box:

   * To create a new user account, highlight *[NEW]*.

   * To model a new account after an existing account, highlight the existing account. The new account will have the same privilege and group membership as the selected account. You can change the account permissions later.

4. Select the *Add* command button.

   The *Add User Account* dialog box appears. (Figure 6-2.)

   If you selected an existing account, some of the text boxes in this dialog box are already filled in.

5. Enter information into the text boxes of the *Add User Account* dialog box as follows:

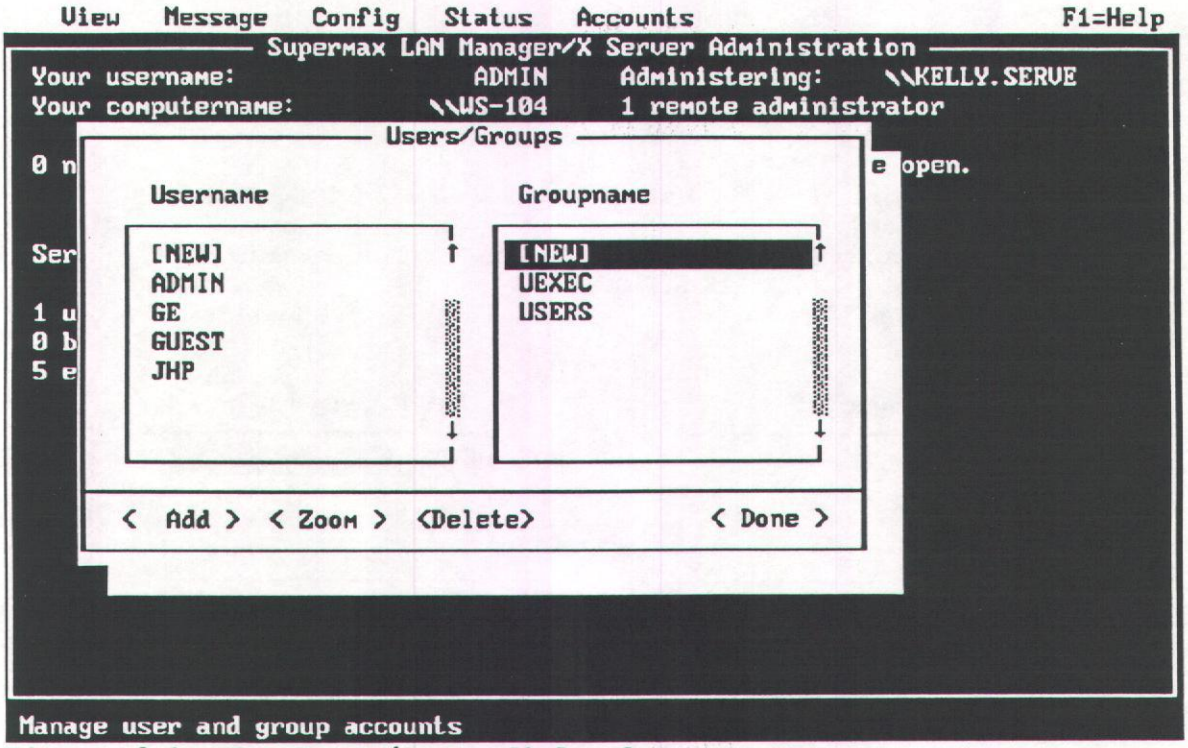


Figure 6-1. The *Users/Group* dialog box

a) At the *Username* text box, supply the username for the new user. Usernames can be a maximum of 20 characters long and may be composed of alphanumeric (a-z, A-Z, 0-9) and the following special characters:

$ % - _ @ { } ~ ‘ ! # ( ).

Do not use special national characters. Usernames are case insensitive, provided they do not include æ, ø, and å which are case sensitive.

b) At the *Password* text box, assign a password for the user. The allowable characters for a password are the same as those for a username. The maximum allowable length for a password on a server running user-level security is 14 alphanumeric characters. The minimum allowable length for a password is determined by the value of the *minpassword=* parameter in the *[lmxserver]* section of the server's *lanman.ini* file. (For more information about this parameter, see Chapter 9, *Changing the Default Server Configuration.*)

c) At the *Directory* text box, type a name for the user's home directory on the server. The name you type may have up to 8 alphanumeric characters. Often, administrators enter the username in this text box, so that the home directory name and the username are the same.

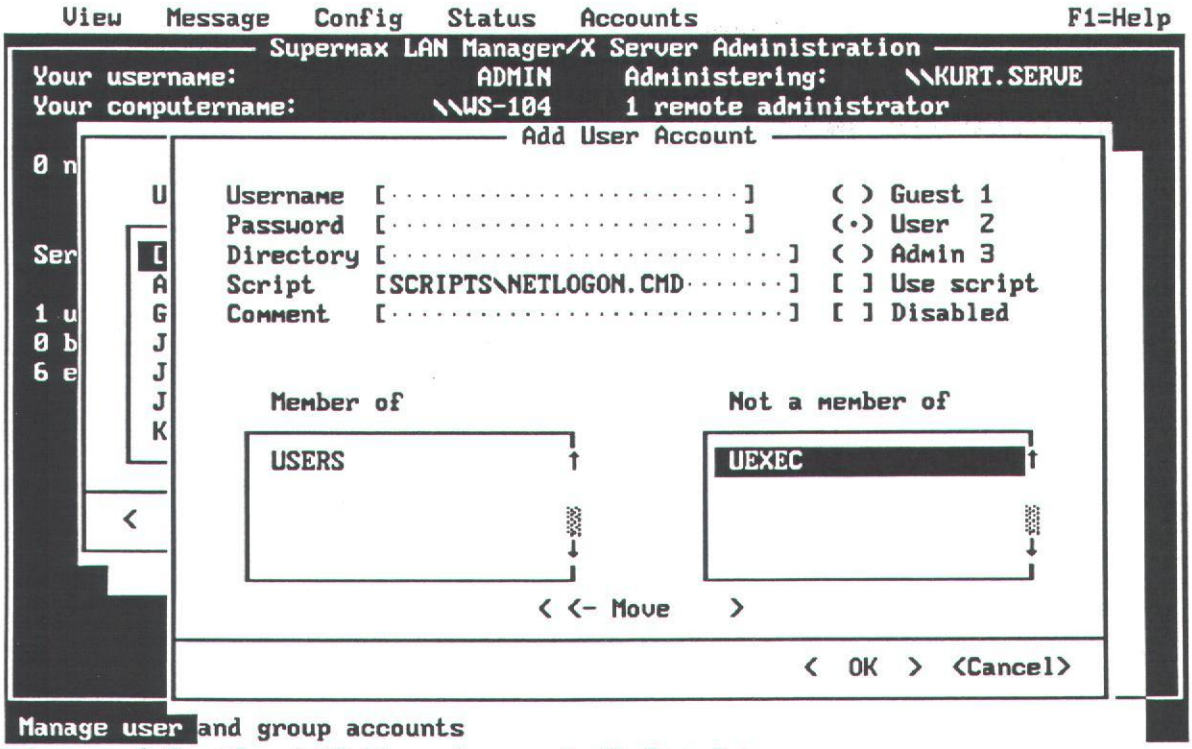


Figure 6-2. The *Add User Account* dialog box

A home directory is a private disk storage area on the server for this particular user. Home directories are optional. Supermax LAN Manager/X creates home directories as subdirectories of the */usr/lanman* directory (unless the server has a */usr2* file system; if that is the case, the user's home directory is created in the */usr2/lanman* directory).

Note: If logon validation is disabled and you want to allow the user access to his or her home directory, you must create a shared directory and grant the user access to this shared directory. The shared directory must be placed above the user's home directory.

If you leave this text box blank, the user will not have a home directory. This will not affect the user's ability to access server resources.

Note: You can specify a different default location for all users' home directories by altering the value of the *userpath=* parameter in the *[server]* section of the server's *lanman.ini* file. For instructions on how to change this parameter, see Chapter 9, *Changing the Default Server Configuration*.

d) The Script text box entry is based on whether or not this server performs logon validation. If this server will validate logon requests by this user, you can optionally have a script run when the logon request is validated. This text box entry is used to specify the script that will be run.

* If you enter only a filename (without a path), the system puts the script file in the */usr/lanman/scripts* directory (if the server has a */usr2* file system, the system puts the script file in the */usr2/lanman/scripts* directory).

  - For Basic DOS and Enhanced DOS clients, the default script is contained in the *netlogon.bat* file.

  - For OS/2 clients, the default script is contained in the *netlogon.cmd* file.

  Caution: If the *Use script* check box is not marked, this server will not perform logon validation for this user, nor will it run the logon script. In addition, this user will not be able to access this server.

  For more information about logon scripts, see Appendix B, *Managing Logon Validation*.

  - If this server is not a logon validator, leave the text box empty. Press the TAB key to move to the next text box. Proceed to Step e.

e) At the *Comment* text box, type a descriptive comment identifying this user. This remark can be up to 48 characters long, though the LAN Manager text boxes will not show the entire remark. A typical comment might be the user's full name and phone number. This comment is seen only by administrators of this server.

6. Use the TAB key to move to the column of option buttons on the right of the *Add User Account* dialog box. Select the privilege level for this user (using either the arrow keys or the left mouse button): *admin*, *user*, or *guest*.

7. Mark or unmark the following check boxes as needed:

   Note: To mark a check box, either press the Spacebar once, or, if you are using a mouse, click the left mouse button.

   * *Use script*
   If this server is a logon validator (running logon validation) and you want it to be able to validate this user's logon requests, mark this check box. If this user does not have an account on any other server, and the logon validation is being used on the network, you must mark this check box. Otherwise, the user will not be able to log on to the LAN.

   Note: In the case of distributed logon validation, marking the *Use script* check box does not ensure that this server will validate the user. If other servers have a user account for this username and password, any of those servers may perform logon validation for this user.



If you mark this check box you may also include the pathname of a script in the *Script* text box. The script you specify will run whenever the user successfully logs on to the network.

For more information about running logon scripts, see Appendix B, *Managing Logon Security*.

* *Disabled*
If you want to prevent the user from accessing resources on this server, mark this check box. This is equivalent to temporarily removing this user's account from the server.

8. Use the two list boxes and the *Move* command button to specify the groups to which the user is to belong.

   To make the user a member of a group, highlight the desired group in the *Not member of* list box. Select the *Move* command button.

   To remove the user from membership in a group, highlight the group in the *Member of* list box. Select the *Move* command button.

9. Select the *OK* command button.

   One of the following occurs:

   * If you did not assign a home directory to the user in Step 5c, the user account is added and you are returned to the *Users/Groups* dialog box. You have completed this procedure. Now you need to grant the new user access to LAN resources. To grant a new user account access to disk resources, see Chapter 7, *Managing Shared Directories*. To grant access to print resources, see Chapter 8, *Managing Shared Printers*.

   * If you assigned a home directory to the user in Step 5c, the system displays the *Edit File Permission* dialog box, allowing you to assign access permissions to the home directory. Using access permissions, you can specify which users or groups can access the directory and the operations they can perform (for example, reading or writing to files in the directory). (Figure 6-3.)

10. Select the *Set explicit permissions* option button.

11. Mark or unmark the following check boxes as needed:

    * *Audit this resource*
    If you want to keep track of who uses this home directory, when it is used, and how it is used, mark this check box. To use this feature, the Audit Trail must be enabled on this server (using the *auditing=* parameter in the *[server]* section of

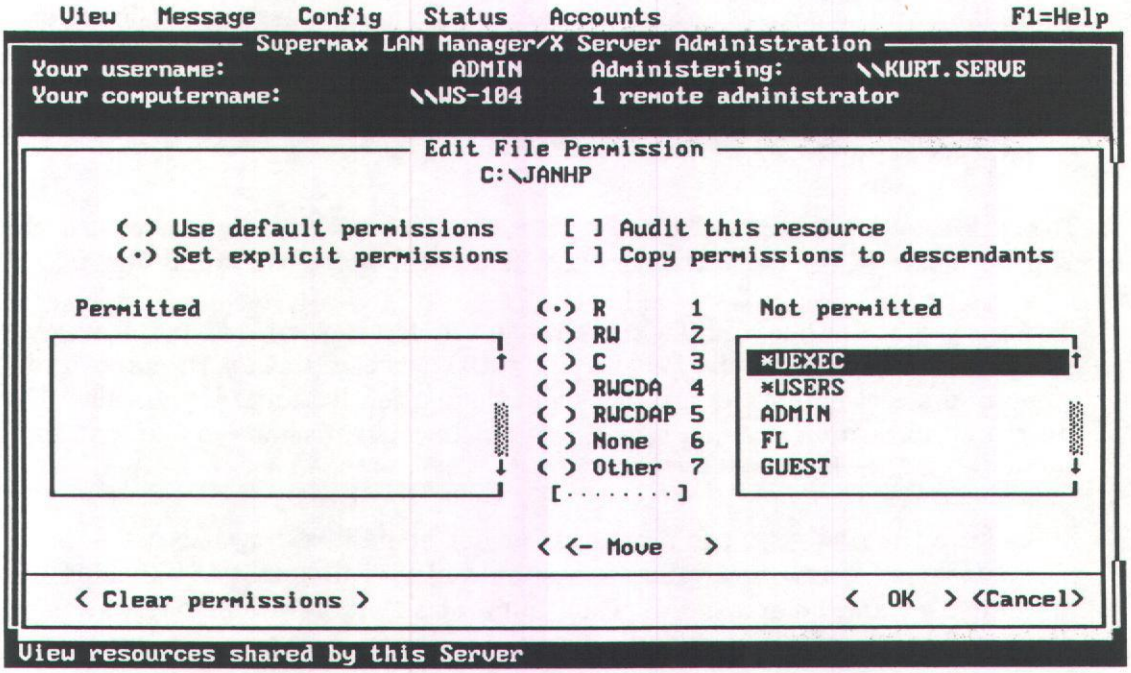


Figure 6-3. The *Edit File Permission* dialog box

the server's *lanman.ini* file). To set the value of this parameter, see Chapter 9, *Changing the Default Server Configuration*.

* *Copy permissions to descendants*
If you want to assign the same access permissions for this home directory to every directory and file below it in the directory hierarchy, mark this check box.

12. Use the two list boxes, the access permission option buttons, and the *Move* command button to specify which users or groups will be permitted to use this home directory. For each user or group that is permitted to access the directory, you can also specify a unique set of access permissions that control what operations the user or group can perform on the home directory (such as reading or writing to files in the directory). If you wish to limit access to only the owner of the home directory, then make that user the only member of the *Permitted* list box.

    Specify access permissions for each user and group as follows:



* To add a user or group to the *Permitted* list box, highlight that username or groupname in the *Not permitted* list box. Specify the access permissions you want that user or group to have, using the access permission option buttons. Then select the *Move* command button. The user or group moves to the *Permitted* list box with the access permissions you specified with the access permission option buttons.

* To remove a user or group from the *Permitted* list box, highlight that username or groupname in the *Permitted* list box. Select the *Move* command button.

* If you make a mistake and wish to change the access permissions for a user or group that is already in the *Permitted* list box, choose that username or groupname and select one of the access permission option buttons. If you select the *Other* option button, you can type a set of access permissions in the text box below the option button.

  Make sure the new user can access his or her home directory. Access permissions on a new home directory should allow full access (*RWCXDAP*) for the new user and no access (*N*) permission for all others. Remember, giving the user the *P* access permission will allow that user to change access permissions for the home directory.

  Home directories are where users should keep private files on the server. As an administrator, you may need to keep an eye on how much disk space the home directories are consuming and issue warnings accordingly.

13. Select the *OK* command button.

14. To add additional users, repeat Steps 2 through 13 for each user.

You have added a user account to the server. Now you need to grant the new user access to LAN resources. To grant a new user account access to disk resources, see Chapter 7, *Managing Shared Directories*. To grant access to print resources, see Chapter 8, *Managing Shared Printers*.

Example
A new user, John, has joined the accounting department and needs to be able to use the *mis.serve* server. As the server administrator, you set up the new account.

Using the Full Screen Net Admin Interface, you access the *mis.serve* server. Next, you select the *Accounts* menu and then select the *Users/Groups* menu item. In the *Users/-Groups* dialog box, you move to the *Username* list box and select *[NEW]*. Then you select the *Add* command button.

In the *Add User Account* dialog box, you begin filling in information. You type the new username, johnoc and moving to the *Password* text box, you type the password given to every new user: `newuser`.

In the *Directory* text box, you type the name of a new home directory on the *mis.serve* server. To simplify administration, you've decided to always give home directories the same name as the user account. In this case, you type `johnoc` which creates the directory */usr/lanman/johnoc*.

The next text box is *Script*. Previously, you created a logon script that establishes some basic connections to printers and central servers for employees using OS/2 clients. This script is in the */usr/lanman/scripts/newuser.cmd* file, so you type `scripts/newuser.cmd` in this text box, since *johnoc* is using an OS/2 client. (If John was using either a Basic DOS or an Enhanced DOS client, you would use the DOS version of this script, called *newuser.bat*.)

In the *Comment* text box, type a remark for this account. Following the pattern of other accounts on the *mis.serve* server, you type in the new user's full name and telephone extension. Pressing the Tab key, you move to the column of option buttons defining privilege level. Since John is a junior accounting clerk with a limited need to access resources, you mark the *Guest* option button. This bars *johnoc* from membership in the *users* group; in the list boxes below, the users groupname moves from the *Member of* to the *Not a member of* list box.

You then move to the *Use script* check box. Since the *mis.serve* server is a central logon validator, you mark this check box. When John logs on, LAN Manager will validate the logon and will run a logon script for him.

The next check box is *Disabled*. Since this is to be an active account, you leave this box unmarked.

Finally, you move to the two list boxes at the bottom of the dialog box. Because of the guest privilege level, *johnoc* cannot be a member of the users group. However, he should be a member of the accounting group so that he can reach the appropriate resources for his job. You move the accounting groupname from the *Not a member of* list box to the *Member of* list box.

The information in this dialog box is now complete; you select the *OK* command button, and a confirmation dialog box appears, asking if it is all right to create the home directory for *johnoc* in the */usr/lanman* directory. You select the *OK* command button to create the directory.

Since LAN Manager is creating a new directory on the *mis.serve* server, it brings up the *Edit File Permissions* dialog box. You see that *johnoc* is in the *Permitted* list box and has full access permissions (*RWCXDAP*). This means that John can do whatever he wants in this directory, even change the access permissions of other users to access this directory. When you select the *OK* command button, you have completed adding this user account.

At this point, you have two responsibilities concerning the new account:

* Give John information about his username, password, and home directory. You should also tell him about changing his password and about the connections that are automatically made for him by the *newuser.cmd* logon script.

* Assign access permissions for John to specific resources. Since *johnoc* is a member of the *accounting* group, John already has access to some resources. If he needs to use other resources, you must give him additional group memberships or modify the access permissions on the relevant resources.

6.2.1.1. Equivalent net Command

You can also add users using the **net user** command. For more information about the **net user** command, see Chapter 10, *Command Directory*.

6.2.2. Changing User Passwords

Although an administrator cannot see a user's password, you can change users' passwords. You may want to change a password under any of these circumstances:

* When users forget their passwords

* When users fail to change their passwords for a long time

* When you need to force a new password for security reasons

Changing a user's password on this server does not change that user's passwords on other servers. If this server is a logon validator, however, changing a user's password can affect the user's access to the LAN.

To change a user's password, follow these steps:

1. Start the Full Screen Net Admin Interface and access the server you wish to administer. (For instructions, see the section entitled *Accessing the Full Screen Net Admin Interface*, in Chapter 3.)

2. Select the *Accounts* menu and select the *Users/Groups* menu item.

   The *Users/Groups* dialog box appears.

3. Highlight a username in the *Username* list box.

4. Select the *Zoom* command button.

   The *Change User Account* dialog box appears. (Figure 6-4).

5. Type the new password for this user in the *Password* text box of this dialog box.

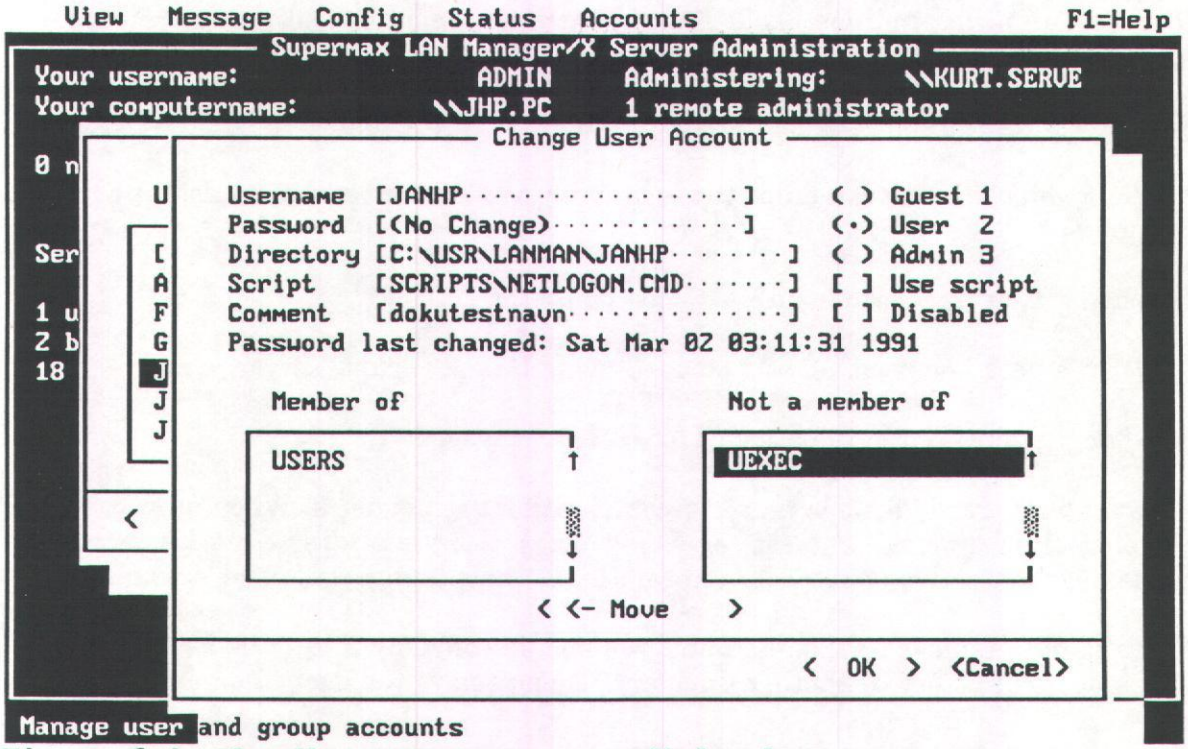


Figure 6-4. The *Change User Account* dialog box

Note: The maximum allowable length for a password on a server running user-level security is 14 alphanumeric characters. The minimum allowable length for a password is determined by the value of the *minpassword=* parameter in the *[lmxserver]* section of the server's *lanman.ini* file. (For more information about this parameter, see Chapter 9, *Changing the Default Server Configuration*.)

6. Select the *OK* command button.

   The *Edit File Permissions* dialog box may appear, letting you change access permissions on the user's home directory (if there is one).

7. Inform the user of the password change.

6.2.2.1. Equivalent net Command

You can also change a user's password using the **net password** command. For more information about the **net password** command, see Chapter 10, *Command Directory*.

6.2.3. Removing User Accounts

This section describes how to remove a user account. It does not describe how to revoke access permissions for access to specific resources. For information about revoking access permissions on disk resources, see Chapter 7, *Managing Shared*



Directories. For information about revoking access permissions on printer resources, see Chapter 8, *Managing Shared Printers*.

You may want to remove a user account under any of the following circumstances:

* When you change a username (by creating a new account and then deleting the old one)

* When a user has permanently stopped using the LAN

* When a user has permanently stopped using this particular server

* When you must close the account for security reasons

You can temporarily disable a user account without removing it. When an account is disabled, the user cannot access server resources. See the *Adding User Accounts* section earlier in this chapter for information on how to disable a user account.

If you plan to remove an user account, you should copy any files to be saved from the user's home directory to another directory. Then remove the user's home directory.

To remove a user account from the server, follow these steps:

1. Start the Full Screen Net Admin Interface and access the server you wish to administer. (For instructions, see the section entitled *Accessing the Full Screen Net Admin Interface*, in Chapter 3.)

2. Select the *Accounts* menu and select the *Users/Groups* menu item.

   The *Users/Groups* dialog box appears.

3. Highlight the username you wish to remove in the *Username* list box.

4. Select the *Delete* command button.

   A dialog box appears, asking you to confirm your decision.

5. Press RETURN to confirm your choice.

6.2.3.1. Equivalent net Command

You can also remove a user account using the **net user** command. For more information about the **net user** command, see Chapter 10, *Command Directory*.

6.2.4. Displaying Existing User Accounts

To display user accounts from the Full Screen Net Admin Interface, follow Steps 1 and 2 of the procedure entitled *Adding User Accounts*, earlier in this chapter.

To display user accounts from the UNIX-system using a terminal connected to your server, type:

```
/usr/net/servers/lanman/mapuser -l
```

This program will list the LAN Manager accounts and their corresponding UNIX system accounts.

Note: You may add, or delete a user accounts from this screen using the Command Line Administration Utility. For more information, see Chapter 5, *Managing Server Operations*.

6.3. Managing Groups

A group is a set of LAN users that have something in common. For simplicity of administration, you can define groups of users and assign them groupnames. A change that is made to the group affects all individual members of the group.

This section contains instructions for performing the following group management tasks:

* Adding new groups by using the Full Screen Net Admin Interface
* Adding members to an existing group
* Managing the UEXEC group
* Removing members from a group
* Removing groups

6.3.1. Adding New Groups Using the Full Screen Net Admin Interface

Groups can simplify your job as administrator. It is easier to keep track of a few groups and their common interests than to keep track of all users and their individual needs. Users don't need to know about groupnames, since groups are used only for server administration and are meaningful only to an administrator.

To add a new group to the server by using the Full Screen Net Admin Interface, follow these steps:

1. Start the Full Screen Net Admin Interface and access the server you wish to administer. (For instructions, see the section entitled Accessing the Full Screen Net Admin Interface, in Chapter 3).

2. Select the *Accounts* menu and select the *Users/Groups* menu item.

The *Users/Groups* dialog box appears.

3. Highlight one item in the *Groupname* list box.

   * Highlight *[NEW]* to create an entirely new group.

   * Highlight an existing groupname if the group you are creating is to be modeled after that existing group. The new group will have the same group members as the highlighted group. You can changed the membership later.

4. Select the *Add* command button.

   The *Add Group Account* dialog box appears. (Figure 6-5).

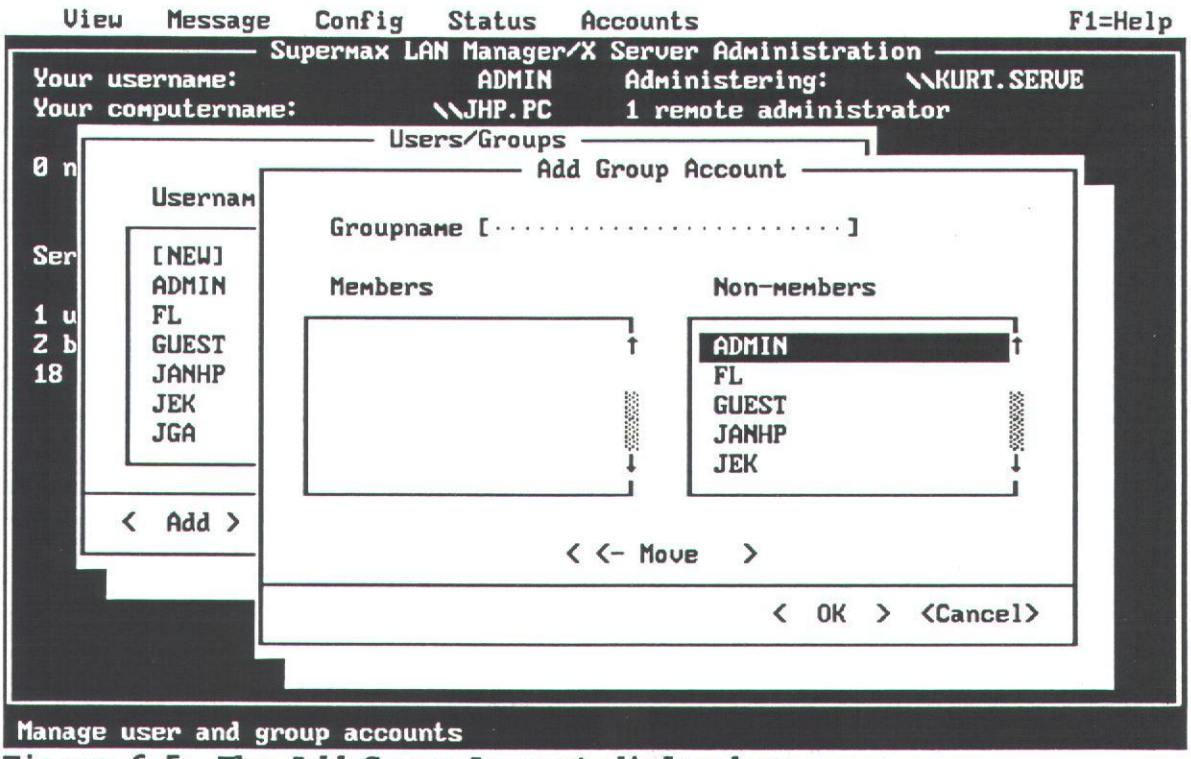


Figure 6-5. The *Add Group Account* dialog box

If you selected *[NEW]* the *Members* list box should be empty; if you selected an existing group, the *Members* list box should have entries. In either case, the usernames of all users who have accounts on this server appear in one of the two list boxes.

5. At the *Groupname* text box, type the name of the new group.

The groupname should be easy to remember and reflect the group's purpose. Groupnames can be a maximum of 20 characters long and may be composed of alphanumeric (a-z, A-Z, 0-9) and the following special characters:

$ % - _ @ { } ~ ‘ ! # ( ).

Do not use special national characters. Groupnames are case insensitive.

6. If you want to specify the members of this group, use the *Move* command button to move them between the *Non-members* list box and the *Members* list box, as desired. To do this, highlight the desired username, then select the *Move* command button. Repeat this step as necessary, until the new user group has the desired members.

7. Select the *OK* command button.

8. To add additional groups, repeat Steps 2 through 7 for each group.

6.3.1.1. Equivalent net Command

You can also add groups to your server using the **net group** command. For more information about the **net group** command, see Chapter 10, *Command Directory*.

6.3.2. Adding Members to an Existing Group

When you add a new user, you may need to include that user in some of the existing groups on the LAN. You can define group memberships when you add the user account (see *Adding User Accounts*), or at a later time. A user can be a member of up to 256 groups, not counting membership in the default *users* and *uexec* groups.

To add members to an existing group, follow these steps:

1. Start the Full Screen Net Admin Interface and access the server you wish to administer. (For instructions, see the section entitled *Accessing the Full Screen Net Admin Interface*, in Chapter 3.)

2. Select the *Accounts* menu and select the *Users/Groups* menu item.

   The *Users/Groups* dialog box appears.

3. In the *Groupname* list box, highlight the name of the group to which you want to add a member.

4. Select the *Zoom* command button.

   The *Change Group Account* dialog box appears. (Figure 6-6).

5. In the *Non-members* list box, highlight the username you want to add as a member of the group.

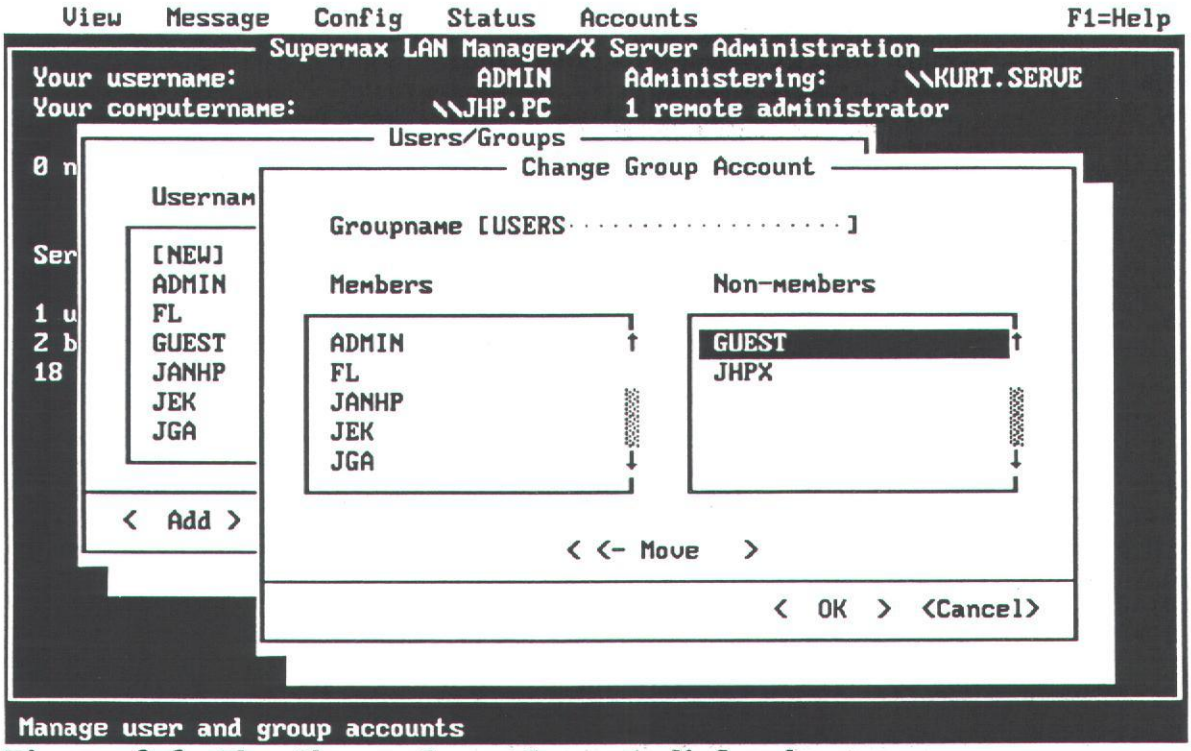


Figure 6-6. The *Change Group Account* dialog box

6. Select the *Move* command button.

7. Repeat Steps 2 through 6 until you are finished adding members to the group.

8. Select the *OK* command button.

Example
Since you created the *lasers* group, the new accounting clerk, John, has been hired in the accounting department. He will need to use the shared laser printer queue to print financial statements. So you must add John's username (*johnoc*) to the *lasers* group. Using the Full Screen Net Admin Interface, you select the *Accounts* menu and the *Users/Groups* menu item. In the *Users/Groups* dialog box, you move into the *Groupname* list box, highlight *lasers*, and select the *Zoom* command button.

In the *Change Group Account* dialog box, you move to the *Non-members* list box, highlight *johnoc*, and then select the *Move* command button. This moves *johnoc* to the *Members* list box. Finally, you select the *OK* command button.

6.3.2.1. Equivalent net Command
You can also add members to a group using the **net group** command. For more information about the **net group** command, see Chapter 10, *Command Directory*.

6.3.3. Managing the uexec Group

The Server Program allows users who are members of the *uexec* group to remotely execute UNIX system commands and programs on the server. Unlike using a terminal emulator to execute UNIX system commands, using the remote execution feature of the *uexec* group maintains the full functionality of a client. Users can execute a UNIX system command from their client's DOS or OS/2 command line, and immediately resume working with a shared directory or application. Remote UNIX system commands can run in the foreground or background and users can monitor and kill commands running in the background. Users execute remote UNIX system processes by invoking the **uexec** command.

When operating in user-level security mode, the LAN Manager server will accept **uexec** requests only if the following conditions are met:

* The user making the request must be a member of the *uexec* group. The *uexec* group is automatically created as a default group account by the Server Program during installation. New users, however, must be manually added to the *uexec* group. To do this, perform the appropriate procedure:

  - To use the Full Screen Net Admin Interface to add users to the *uexec* group, see the procedure in the section entitled *Adding Members to an Existing Group*, p.6-15).

  - To add users to the *uexec* group, from a terminal connected to the UNIX LAN Manager Server use the Command Line Administration Utility and the command **net group uexec** `usernames` **/add**. See the section in Chapter 5 entitled *Running the Command Line Administration Utility* and Chapter 10, *Command Directory*.

* The user must specify an appropriate drive identifier for the **uexec** command's driveid parameter. This drive identifier must be linked to a directory on the server where the user has read, write, create, and delete access permissions (*RWCD*).

  You may wish to create a special directory for this purpose. If so, when creating the directory, you should indicate that it is for **uexec** use in the *Comment* text box. When users list available directories on the server, they will be able to read this comment.

For information concerning the **uexec** command on servers running share-level security, see Appendix A, *Managing Share-Level Security*. For more information about the **uexec** command, see *Supermax LAN Manager/X - User's Guide*.



6.3.4. Removing Members from a Group

You will need to remove a user from a group if you are restructuring groups or if a user no longer needs to belong to a group.

To remove a user from a group, follow these steps:

1. Start the Full Screen Net Admin Interface and access the server you wish to administer. (For instructions, see the section entitled *Accessing the Full Screen Net Admin Interface*, in Chapter 3.)

2. Select the *Accounts* menu and select the *Users/Groups* menu item.

   The *Users/Groups* dialog box appears.

3. In the *Groupname* list box, highlight the groupname of the group you want to change and select the *Zoom* command button.

4. In the *Change Group Account* dialog box, highlight the username you want to remove from the group and select the *Move* command button.

5. Select the *OK* command button.

You have now removed a user from a group. To remove additional users, repeat Steps 1 through 4.

Example

In creating the *lasers* group, you included Jack's username in the group membership, since he was formerly responsible for producing financial statements. But Jack no longer needs access to the laser printers, so you have decided to remove Jack's username (jackst) from membership in the *lasers* group.

Using the Full Screen Net Admin Interface, you select the *Accounts* menu and the *Users/Groups* menu item. In the *Users/Groups* dialog box, you move into the *Groupname* list box, select *lasers*, and select the *Zoom* command button.

In the *Change Group Account* dialog box, you move to the *Members* list box, highlight *jackst*, and select the *Move* command button. This moves *jackst* to the *Non-members* list box. Finally, you select the *OK* command button.

6.3.4.1. Equivalent net Command

You can also remove a member from a group by using the **net group** command. For more information about the **net group** command, see Chapter 10, *Command Directory*.



6.3.5. Removing Groups

Defining groups is a powerful way of keeping the LAN responsive to the needs of its users. Removing a group can have great impact. Before removing a group, consider the consequences and be sure to notify users if it will change their ability to access resources.

To remove a group from the LAN, follow these steps:

1. Start the Full Screen Net Admin Interface and access the server you wish to administer. (For instructions, see the section entitled *Accessing the Full Screen Net Admin Interface*, in Chapter 3.)

2. Select the *Accounts* menu and select the *Users/Groups* menu item.

   The *Users/Groups* dialog box appears.

3. From the *Groupname* list box, highlight the groupname you want to delete and select the *Delete* command button.

   A message box appears, asking you to confirm your decision.

4. Select the *OK* command button.

You have now removed a group from the network.

Example
You have been evaluating some project management software. To solicit opinions, you put the software on the *mis.serve* server, then invited people to use it on a test basis. To control access to the software, you defined a group named *project*. Now your evaluation is complete and you want to remove the project group.

Using the Full Screen Net Admin Interface, you select the *Accounts* menu and the *Users/Groups* menu item. In the *Users/Groups* dialog box, you move into the *Groupname* list box, highlight *project*, and select the *Delete* command button. You confirm the choice by choosing the *OK* command button, and the project *group* is removed from the server.

6.3.5.1. Equivalent net Command

You can also remove a group using the **net group** command. For more information about the **net group** command, see Chapter 10, *Command Directory*.

7. Managing Shared Directories

7.1. Overview

The Server Program lets you control access to a server's directories. You can share the root directory on the server's hard disk, or any and all subdirectories on the disk. This chapter describes how to manage access to a server's shared directories, including:

* Listing Shared Directories
* Sharing Directories
* Managing Disk Resource Access Permissions
* Unsharing Directories
* Maintaining a Shared Disk

For information about using shared disk devices, see *Supermax LAN Manager/X - User's Guide*.

7.2. Listing Shared Directories

Listing the directories shared by a server lets you see which of the server's directories are available to the network. Before sharing a new directory from the server, you should first check to see which directories (and sharenames) are currently shared.

You can list the shared directories on a server by using either the Full Screen Net Admin Interface or the Command Line Net Interface.

7.2.1. Listing Shared Directories by Using the Full Screen Net Admin Interface

From an Enhanced DOS or OS/2 client, you can list the shared directories for your server. To do so, follow these steps:

1. Start the Full Screen Net Admin Interface and access the server you wish to administer. (For instructions, see the section entitled *Accessing the Full Screen Net Admin Interface*, in Chapter 3.)

2. Select the *View* menu and select the *This server* menu item.

   The *Resources This Server Is Sharing With the Network* dialog box appears.

   The list box in this dialog box shows the sharename, path, and a remark for each shared directory.

3. To see more information about a shared directory, select that directory from the list box and select the *Zoom* command button.

   The *Shared Resource Information* dialog box appears.

   This dialog box repeats the information in the *Resources This Server Is Sharing With the Network* dialog box as well as the maximum number of users that can use this directory and a list of users currently using the directory.

4. Select the *Done* command button to return to the *Resources This Server Is Sharing With the Network* dialog box.

5. Select the *Done* command button to return to the background screen.

7.2.2. Listing Shared Directories by Using the Command Line Net Interface

You can also list the shared directories for your server using the Command Line Net Interface. If you do it from a client, type

```
net view \\servername
```

or

```
net admin \\servername /c net share
```

where *servername* is the name of the server.

If you do it from a UNIX system promt at the server console or using the Command Line Administration Utility, type

```
net share.
```

7.3. Sharing Directories

You can use LAN Manager to share some or all of a server's disk directories. You can also specify what individual users can or cannot do with a directory's contents. For example, you could allow one group of users to read files in a directory, but not write to them, while allowing another group to write information to existing files but not to create new ones. For information about assigning disk resource access permissions, see the next section, *Managing Disk Resource Access Permissions*.

By sharing a server's directories, you can share data and programs with a number of people on the local area network. This ensures that all users have access to the same copy of the data or programs in the shared directory. It also saves overall disk space by eliminating the need for duplicate copies of files on everyone's computer.

Sharing directories saves time. When users use shared directories to access files over the local area network, they no longer have to walk to another computer to look at a file or copy it to a diskette.

Sharing directories also makes it possible for users to archive files on a server's hard disk rather than on floppy disks. Hard-disk storage is generally more reliable than diskette storage.

Since many users will depend on the server's shared directories, it is recommended that you periodically back up the server's hard disk. For instructions, see the section entitled, *Backing Up and Restoring Server Files*, later in this chapter.

Important: When the Server Program is started, default directories (on the UNIX system) are established to function as the location for creating new shared directories on the server. When you are creating a new shared directory, you must specify its location on the server (using the path text box). If the path text box contains a directory that does not already exist, the Server Program will attempt to create that directory in the location you specified. It is recommended that you place new shared directories under one of the default administerable LAN Manager directories (such as the *c:\usr\lanman* or *c:\usr2\lanman* directories). For more information about specifying the proper path for a shared directory, refer to the section entitled *Recommended Locations for Creating New Shared Directories*, in Chapter 4.

Procedure
To share a directory, follow these steps:

1. Start the Full Screen Net Admin Interface and access the server you wish to administer. (For instructions, see the section entitled *Accessing the Full Screen Net Admin Interface*, in Chapter 3.)

2. Select the *View* menu and select the *This server* menu item.

   The *Resources This Server is Sharing With the Network* dialog box appears. This dialog box displays all resources currently being shared from the server.

3. Select the *Add share* command button.

   The *What would you like to share?* dialog box appears.

4. Select the *Disk* directory option button.

   The *Share a Disk Resource With the Network* dialog box appears. (Figure 7-1).

5. Enter information into the text boxes of the *Share a Disk Resource With the Network* dialog box as follows:

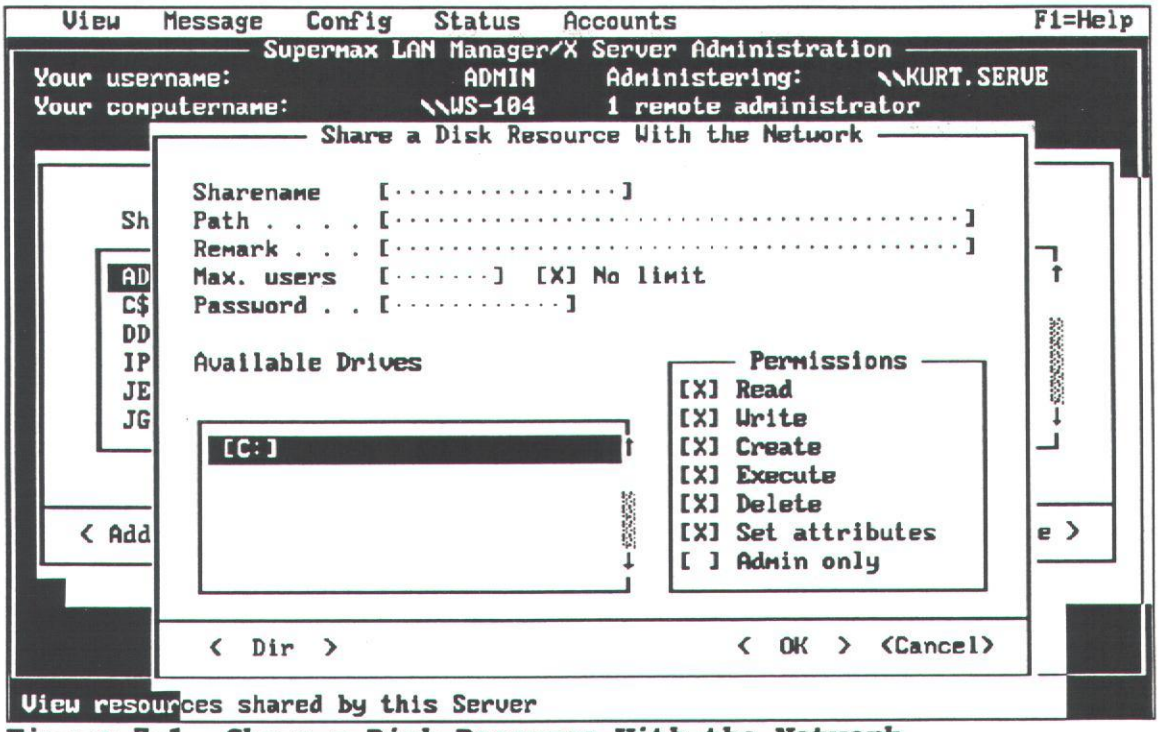


Figure 7-1. *Share a Disk Resource With the Network*

a) At the *Sharename* text box, type the sharename for the directory being shared. This is the shared resource name that users will link to when they need to access the directory's contents.

Sharenames for directories can contain a maximum of 8 alphanumeric characters.

b) At the *Path* text box, type the drive letter and path of the server directory you are sharing.

The format of the path statement is as follows:

```
driveid:\directory\subdirectory
```

Where *driveid* is the drive (usually *C*: for the server's hard disk) where the shared directory is stored; and *\directory\subdirectory* is the UNIX system pathname for the shared directory (note the use of backslashes between directory names).

If you specify a path that contains a directory that does not exist, LAN Manager will attempt to create that directory. In such cases, you should specify a path that starts with the default administerable LAN Manager directories (such as the *c:\usr\lanman* or *c:\usr2\lanman* directories). For more information about specifying the proper path, refer to the section entitled *Recommended Locations for Creating New Shared Directories*, in Chapter 4.

c) At the *Remark* text box, type a comment describing the directory.

d) Do *one* of the following:

* At the *Max. users* text box, type the maximum number of users that will be able to access the directory simultaneously. For example, this number may be determined by the software license agreement of a network application program that will be stored in the directory. Such license agreements can specify the maximum allowable number of simultaneous users.

* At the *No limit* check box, mark the check box if you do not wish to limit the number of users that will be able to access the directory simultaneously.

e) Do *one* of the following:

* If the server is running user-level security, proceed to Step f.

* If the server is running share-level security, in the *Password* text box, type a password for the directory. On servers running share-level security, passwords may contain up to 8 alphanumeric characters. The minimum allowable length for a password is determined by the value of the *minpassword=*-parameter in the *[lmxserver]* section of the server's *lanman.ini* file (for more information about this parameter, see Chapter 9, *Changing the Default Server Configuration*).

  Then move to the *Permissions* check boxes. Use these check boxes to assign access permissions for the directory.

f) Select the *OK* command button.

6. Do *one* of the following:

* If the server is running share-level security, the system returns you to the background screen. You have completed this procedure.

* If the server is running user-level security, the *Edit File Permission* dialog box appears. (Figure 7-2).

7. Specify which users and groups can access the new shared directory and what kind of access permissions they will have. For each user or group that is permitted to access the shared directory, you can specify a unique set of access permissions that control what operations the user or group can perform on the shared directory (such as reading or writing to files in the directory). If you wish to limit access to only one user, then make that user the only member of the *Permitted* list box.

   Assign access permissions for the new shared directory as follows:

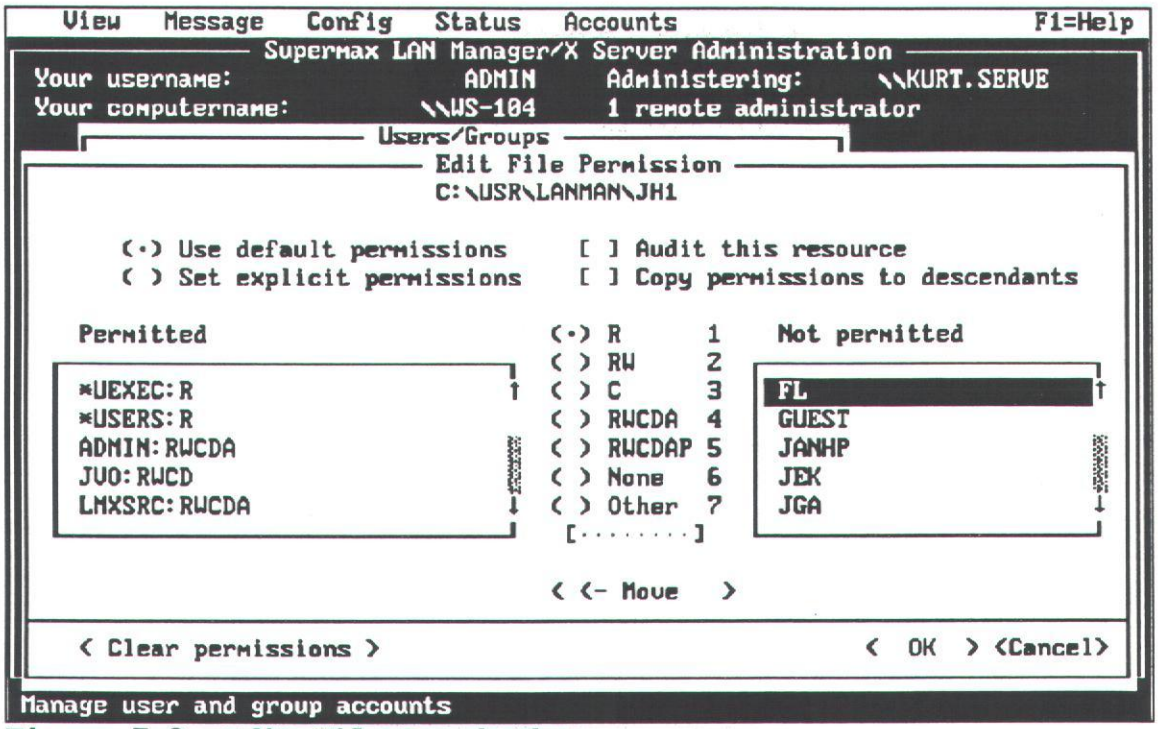


Figure 7-2. *Edit File Permission*

* Determine whether or not you wish to assign the system's default access permissions to the users and groups that will access the shared directory:

  - If you wish to assign the system default access permissions to users and groups that will access the shared directory, select the *Use default permissions* option button.

    Note: You will not be able to use default access permissions if the new shared directory is a subdirectory of other shared directories that are configured for explicit access permissions.

* If you wish to assign access permissions manually for the users and groups that will access the shared directory, select the *Set explicit permissions* option button.

  There are two ways to assign explicit access permissions:

  - To assign the same access permissions to many users and groups, first specify the desired access permission by selecting the proper option button. Then move the users and groups from the *Not permitted* list to the *Permitted* list by highlighting the user or group and selecting the *Move* command button.

- To assign different access permissions to various users and groups, first move the users and groups from the *Not permitted* list to the *Permitted* list by highlighting the user or group and selecting the *Move* command button. Then assign access permissions individually, by highlighting the user or group in the *Permitted* list and then assigning the desired access permis sion by selecting the proper option button.

* Mark the *Audit this resource* check box if you want to record who uses this shared directory, when it is used, and how it is used. To use this feature, the Audit Trail must be enabled on this server (using the *auditing=* parameter in *[server]* the section of the server's *lanman.ini* file). To set the value of this parameter, see Chapter 9, *Changing the Default Server Configuration*.

* Mark the *Copy permissions to descendants* check box if you want to assign the same access permissions that apply to this directory to every directory and file below it in the directory hierarchy.

* Select the *Clear permissions* command button if you wish to remove the access permissions that have been assigned to the shared directory.

8. Select the *OK* command button.

   The system closes the *Edit File Permission* dialog box. The *Resources This Server is Sharing With the Network* dialog box appears. The sharename for the shared directory you just created should appear in the display.

9. Determine whether or not you want to share additional directories:

   * To share additional directories, repeat Steps 2 through 8 for each directory you want to share.

   * To close the *Resources This Server Is Sharing With the Network* dialog box, select the *Done* command button.

Example
You need to create a shared directory for your company's Public Relations staff. Since Public Relations is a fairly security-minded department, you decide to create and share the directory on the *mis.serve* server, a server running user-level security. This allows the Public Relations people to assign different access permissions for different users of the shared directory.

Using the Full Screen Net Admin Interface, you access the *mis.serve* server. You select the *View* menu and select the *This server* menu item. In the *Resources This Server is Sharing With the Network* dialog box, you select the *Add Share* command button. Then, in the *What would you like to share?* dialog box, you select the *Disk directory* option button.



In the *Share a Disk Resource With the Network* dialog box, you start to fill in the text boxes. First, you share the directory with the sharename *pubrel*. This means that members of the Public Relations staff will be able to connect to the shared directory by specifying the pathname `\\mis.serve\pubrel`. You type `c:\usr2\lanman\pubrel` in the *Pathname* text box to tell the Server Program where to find the directory on the server's hard drive (if this directory did not already exist, you would be prompted to approve the creation of a new directory; in response, you would answer *yes*).In the *Remark* text box you type `Public Relations`.

Since the *mis.serve* server is running user-level security, there's no need to specify a password, as would be necessary were the server running share-level security. Finally, in the last text box you set the maximum number of users at 20 (there are 15 people in the Public Relations department right now, so 20 gives them some flexibility).

When you select the *OK* command button, the *Edit File Permission* dialog box appears on the screen. You select the *Set explicit permissions* option button, and mark the *Copy permissions to descendants* check box, ensuring that the access permissions for the *pubrel* directory will apply to all subdirectories and files created by the Public Relations department. Using the list boxes, access permission option buttons, and the *Move* command button, you specify the *Yes* access permission for the *pubrel* directory, thereby giving users read, write, create, delete, and change attribute access permissions. You select the *OK* command button, establishing the access permissions for the directory.

7.3.1. Equivalent net Command

You can also share directories using the **net share** and **net access** commands. For more information about these commands, see Chapter 10, *Command Directory*.

7.4. Managing Disk Resource Access Permissions

This section provides the following information concerning disk resource access permissions:

* Understanding disk resource access permissions
* Looking at access permissions
* Changing access permissions for disk resources
* Changing access permissions as a non-administrative user
* Assigning default and inherited access permissions

7.4.1. Understanding Disk Resource Access Permissions

A disk resource is a disk drive, a directory, or a file. Access permissions that can be assigned to a disk resource appear below:



Create (C) Allows a user to create files and directories within the shared disk resource. The **C** access permission does not grant read or write access to existing files (each of these operations require their own access permissions). After creating a file, a user can read or write to that file only while it is initially opened. Once closed, the user will be unable to open it again.

Delete (D) Allows a user to delete files and directories within the disk resource (but not to delete the disk resource itself).

Read (R) Allows a user to read or open files and to change directories.

Write (W) Allows a user to write to a file.

Execute (E) Allows a user to open a file for execution.

Note: If you assign **R** access permission, you do not need to assign **X** access permission. If you assign **X** access permission without **R** access permission, OS/2 clients can execute the file but not read it, while DOS clients cannot read or execute the file.

Change Attributes (A) Allows a user to change the DOS or OS/2 physical file attributes. These file attributes take precedence over LAN Manager access permissions.

Change Permissions (P) Allows a user to change the LAN Manager access permissions for the resource.

Yes (Y) An abbreviation for the **RWCDA** group of access permissions.

No (N or none) Prevents a user from doing anything. For disk resources, the **N** access permission is sometimes indicated by a colon with nothing after it; you do not actually see the letter *N*. When you assign this access permission, you cannot assign any other access permissions. Use this access permission to exclude individual users from access despite their group memberships.

For example, if you give read and write access permissions to the *users* group, you can exclude a specific user in the *users* group by assigning that user the **N** access permission. The **N** access permission should not be assigned to groups. When evaluating group access permissions, LAN Manager considers the union of all applicable group access permissions.



For example, if you give **RWC** access permission on a directory to the *users* group, but **N** access permission to the *laser* group, members of the *laser* group could still use the directory if they were also members of the *users* group. Assigning **N** access permission to a group does not guarantee that all users of that group will be denied access to the resource.

The Full Screen Net Admin Interface provides convenient groupings of these access permissions, so that you can easily assign common combinations of access permissions. Some of these commonly used combinations include **RWX** (read, write, and execute) and **RWXCDA** (read, write, execute, create, delete, and change attributes).

7.4.2. Looking at Access Permissions

When you share resources under user-level security, you should assign access permissions for each resource. You may need to review the assigned access permissions under the following circumstances:

* Users cannot access resources they need

* Unauthorized users are accessing a resource

To look at the access permissions for a disk resource, follow these steps:

1. Start the Full Screen Net Admin Interface and access the server you wish to administer. (For instructions, see the section entitled *Accessing the Full Screen Net Admin Interface*, in Chapter 3.)

2. Select the *Accounts* menu and select the *File permissions* menu item to look at access permissions for a disk resource.

   The *File Access Permissions For* dialog box appears. (Figure 7-3).

   Use the list box and the *Dir* command button to move through the directories of the server until you find the desired disk resource.

3. When you have found the drive, directory, or file that you want to examine (either in the list box or by typing its pathname in the text box), select the *Zoom* command button to look at access permissions.

   The *Edit File Permission* dialog box appears. The *Permitted* list box shows all users and groups with access permissions for this resource. Each entry is of the form

   ```
   name:permissions
   ```

   where *name* is the username or groupname, and *permissions* specifies the access permissions assigned.

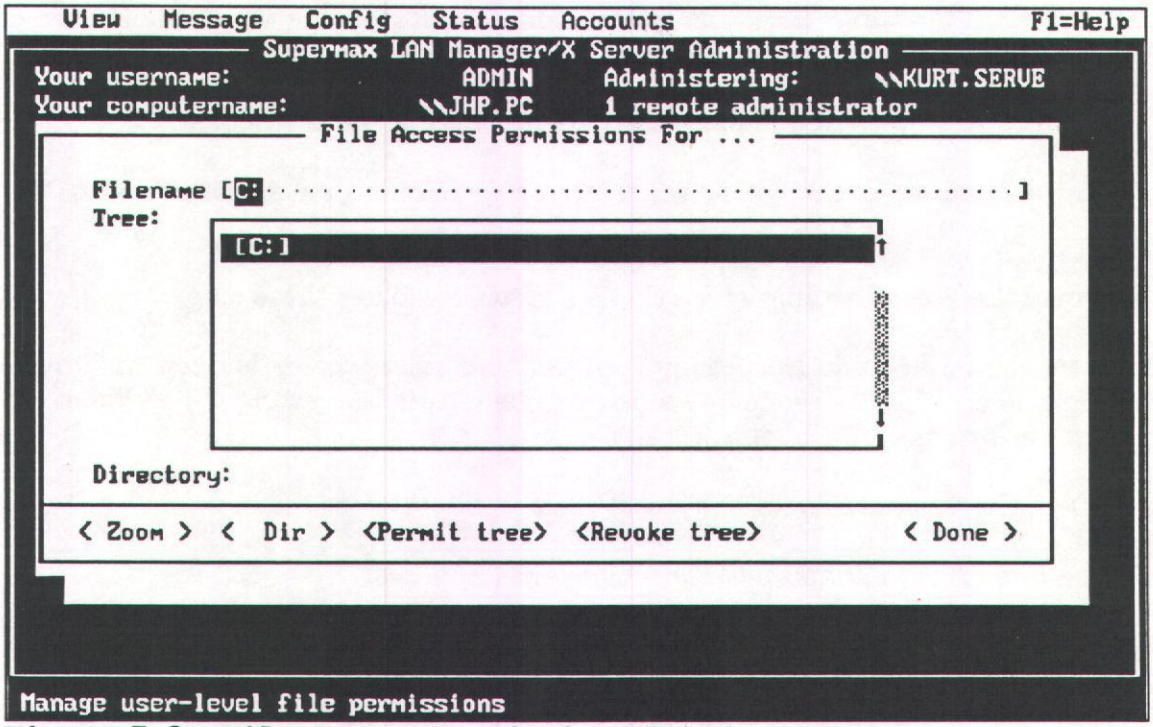


Figure 7-3. *File Access Permissions For*

4. Select the *Cancel* command button to leave this dialog box without making changes.

A user whose name does not appear in the *Permitted* list box can only use the disk resource under the following conditions:

* The user has admin privilege on the server

* The user belongs to a group that is permitted to use the resource

7.4.3. Changing Access Permissions for Disk Resources

Under user-level security, LAN Manager maintains a database of access permissions for disk resources regardless of whether those resources are being shared at any given time. Thus, if you stop sharing a resource and then decide later to start sharing it again, LAN Manager remembers the access permissions you have previously assigned for that resource. Every resource starts with default access permissions; if you change those default access permissions, they remain changed until you change them again. For a description of default access permissions, see the section entitled, *Assigning Default and Inherited Access Permissions*, later in this chapter.

The Full Screen Net Admin Interface automatically asks you to assign access permissions when you share a directory or create a new home directory for a user account. You must assign access permissions for each drive or directory, or else accept the default access permissions.

You may want to change access permissions for a disk resource under the following circumstances:

* You want to stop using the default access permissions for a resource

* You want to assign, change, or delete access permissions for a user or group

Procedure
To change the access permissions for a disk resource, follow these steps:

1. Start the Full Screen Net Admin Interface and access the server you wish to administer. (For instructions, see the section entitled *Accessing the Full Screen Net Admin Interface*, in Chapter 3.)

2. Select the *Accounts* menu and select the *File permissions* menu item.

   The *File Access Permissions For...* dialog box appears.

3. Use the list box and the *Dir* command button to move through the directories of the server until you find the desired disk resource. When you have found the drive, directory, or file that you want to examine (either in the list box or by typing its pathname in the text box), select the *Zoom* command button.

   The *Edit File Permission* dialog box appears. (Figure 7-4).

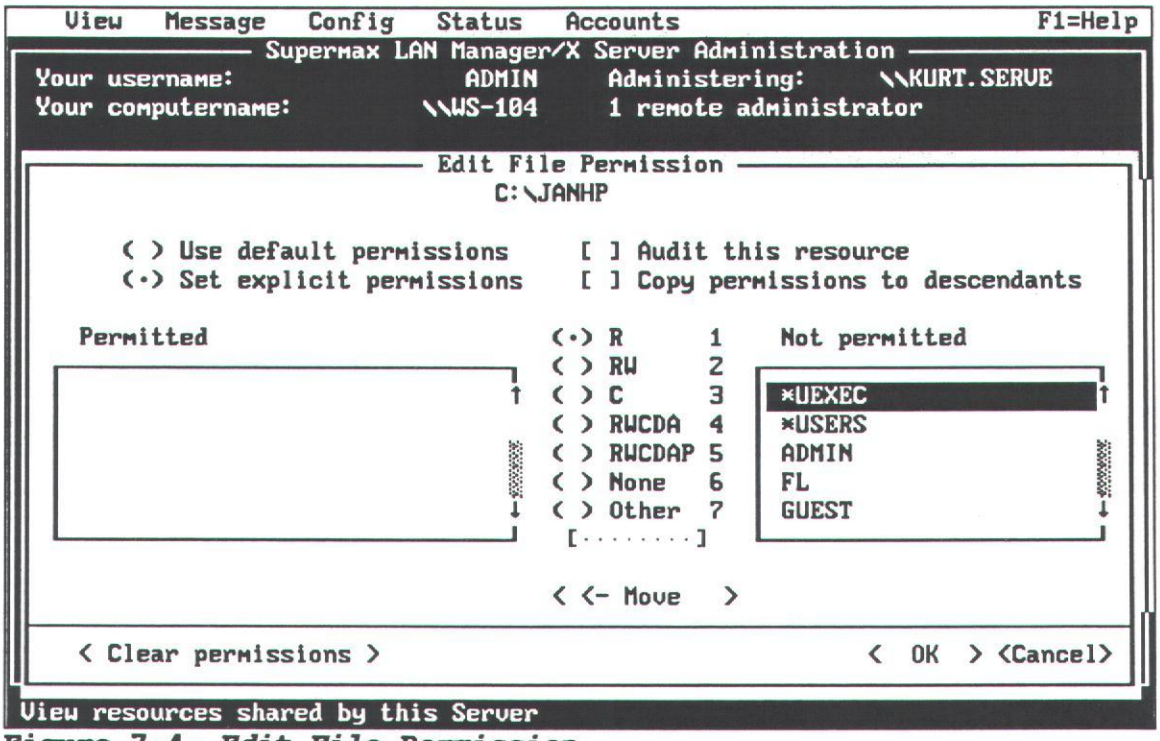


Figure 7-4. *Edit File Permission*

4. Do *one* of the following:

   * If you want to customize access permissions for each user and group, select the *Set explicit permissions* option button. Then proceed to Step 5.

   * If you want to use default access permissions, see *Assigning Default and Inherited Access Permissions* (p.7-14). Then select the *Use default permissions* option button and proceed to Step 5.

   * If you want to remove all current access permissions, select the *Clear permissions* command button. Then proceed to Step 5.

5. Mark or unmark the following check boxes as needed:

   * *Audit this resource*
     If you want to keep track of who uses this resource, when it is used, and how it is used, mark this check box. To use this feature, the Audit Trail must be enabled on this server (using the *auditing=* parameter in the *[server]* section of the server's *lanman.ini* file). To set the value of this parameter, see Chapter 9, *Changing the Default Server Configuration*.

   * *Copy permissions to descendants*
     If you want to assign the same access permissions for this resource to every directory and file below it in the directory hierarchy, mark this check box. For more information on inherited access permissions, see the section entitled *Assigning Default and Inherited Access Permissions*, later in this chapter.

6. Use the two list boxes, the access permission option buttons, and the *Move* command button to specify the access permissions for each user and group as follows:

   * To *add* a user or group to the *Permitted* list box, select that username or groupname from the *Not permitted* list box and select the *Move* command button. The user or group moves to the *Permitted* list box with whatever access permissions are currently selected among the access permission option buttons.

   * To *remove* a user or group from the *Permitted* list box, select that username or groupname and select the *Move* command button. The user or group moves to the *Not permitted* list box.

   * To *change* the access permissions for a user or group in the *Permitted* list box, select that username or groupname and select one of the access permission option buttons. If you select the *Other* option button, you can type a set of access permissions in the text box below the option button.

7. Select the *OK* command button.



Example
You are the *mis.serve* server administrator. You need to change the access permissions for the *c:\usr2\lanman\accounts* shared directory, to allow access to the accounting group. The accounting group's members should be able to read or write to existing files in the directory.

First you invoke the Full Screen Net Admin Interface and access the server you wish to administer. Then, from the *Accounts* menu, you select the *File permissions* menu item. The *File Access Permissions For* dialog box appears. In the *Filename* text box, you type `c:\usr2\lanman` and select the *Dir* command button. This displays the contents of the *lanman* directory in the *Tree:* list box.

You highlight the *accounts* directory in the *Tree:* list box and select the *Zoom* command button. In the *Edit File Permission* dialog box, you select the *RW* option button, then move the accounting group from the *Not permitted* list box to the *Permitted* list box. You finish by selecting the *OK* command button. The accounting group now has **RW** access permissions for the *accounts* directory.

7.4.4. Equivalent net Command

You can also change the access permissions for a disk resource by using the **net access** command. For more information about the **net access** command, see Chapter 10, *Command Directory*.

7.4.5. Changing Access Permissions as a Non-Administrative User

When you give the **P** access permission to a user, you allow that user to change access permissions on a disk resource. This is very different from granting administrative privilege. Someone with admin privilege can change access permissions on any resource, while a user with the **P** access permission can change access permissions only on the specific resource for which you grant the **P** access permission.

Typically, the **P** access permission is only assigned to a non-administrative user when the shared resource is the user's own home directory. If you give a non-administrative user the **P** access permission for a shared resource, be sure to explain the access permission to the user.

7.4.6. Assigning Default and Inherited Access Permissions

Every drive, directory, or file on a server must have a set of access permissions. If you do not explicitly set access permissions for a resource (file or directory), then that resource has default access permissions. Default access permissions are determined by certain other access permissions that you have set.

The Server Program uses a series of tests to determine the default access permissions for a disk resource:

* If the resource is a disk drive, it cannot use default permissions (the *c:* resource must have explicit permissions assigned to it). Every disk drive starts with a null (blank) set of explicit access permissions.



* If the resource has explicit access permissions, the Server Program uses those access permissions.

* If the resource has a parent that has explicit access permissions, the Server Program uses those access permissions. The parent of a file is the directory in which the file is located. The parent of a directory is the next higher directory (if one exists).

* If the parent has no explicit access permissions, use the access permissions for the drive on which this resource is located.

Some of the effects of these rules include the following:

* Any explicit access permissions that you set for any disk resource override default access permissions that you set for the disk drive.

* If a directory does not itself have explicit access permissions, then any file or subdirectory in that directory takes default access permissions from the drive. This is true even if the directory itself takes default access permissions from its parent.

* If you give anyone with *guest* privilege explicit access permissions at the drive level, you must be careful to exclude that user with the **N** access permission from any sensitive resource on that drive. This is tricky because you might assign the **N** access permission to the *users* group for a resource, thinking that this excludes all users, when *guest* users are still able to access the resource (since they are not members of *users*).

* When you create a directory for any purpose, you should assign explicit access permissions to it if you want it to have something other than default access permissions.

If you want to avoid default access permissions, you can assign *inherited access permissions* for an entire directory tree (a directory plus all of its files and subdirectories). Inherited access permissions are access permissions given to each file and subdirectory under a particular directory. If you later add subdirectories or files to this directory, they will *not* inherit these access permissions unless you reset inherited access permissions for the entire tree.

Note: When new directories are created on the server, new subdirectories of these directories take on the same access permissions as their "parent" directory. This does not apply to files, however.

Procedure

To set inherited access permissions for a disk resource, follow these steps:

1. Start the Full Screen Net Admin Interface and access the server you wish to administer. (For instructions, see the section entitled *Accessing the Full Screen Net Admin Interface*, in Chapter 3.)

2. Select the *Accounts* menu and select the *File permissions* menu item.

   The File Access Permissions For... dialog box appears.

3. Use the list box and the *Dir* command button to move through the server's directories until you find the directory you want, or type the pathname of the directory in the *Filename* text box.

4. Select the *Zoom* command button to examine the existing access permissions for this resource.

   The *Edit File Permission* dialog box appears. When you're ready to continue, you can return to the *File Access Permissions For...* dialog box by pressing ESC.

Note: You can assign inherited access permissions from the *Edit File Permission* dialog box by marking the *Copy permissions to descendants* check box. This performs the same action as the *Permit tree* command button in the *File Access Permissions For...* dialog box.

5. Do *one* of the following:

   * If you do not wish to change access permissions for the directory and its descendants, select the *Done* command button to return to the background screen.

   * If you wish to assign the current access permissions for this directory to all of the directory's descendants, select the *Permit tree* command button. Select the *Done* command button to return to the background screen.

   * If you want to remove access permissions for the entire directory tree (no matter how those access permissions were assigned), select the *Revoke tree* command button. Select the *Done* command button to return to the background screen.

Example
You want to assign the accounting group **RW** access permission for all subdirectories and files in the *c:\usr2\lanman\accounts* directory.

You start the Full Screen Net Admin Interface and access the appropriate server. From the *Accounts* menu, you select the *File permissions* menu item. The *File Access Permissions For...* dialog box appears. In the *Filename* text box, you type *\usr2\lanman* and select the *Dir* command button. The contents of the *lanman* directory are displayed. In the *Tree:* list box, you highlight the *accounts* directory and select the *Zoom* command button.

Since you are satisfied with the access permissions assigned to the *accounts* directory, you press ESC and return to the *File Access Permissions For...* dialog box. To assign the *accounts* directory's current access permissions to all of its descendant files and directories, you select the *Permit tree* command button. To return to the background screen, you select the *Done* command button.

7.4.7. Equivalent net Command

You can also assign inherited access permissions for a resource using the **net access** command. For more information about the **net access** command, see Chapter 10, *Command Directory*.

7.5. Unsharing Directories

You may occasionally need to stop sharing a directory. This might be necessary when a shared directory is no longer being used and you want to delete it, or when a project requiring the use of shared files is completed.

To stop sharing a directory, follow these steps:

1. Start the Full Screen Net Admin Interface and access the server you wish to administer. (For instructions, see the section entitled *Accessing the Full Screen Net Admin Interface*, in Chapter 3.)

2. Select the *View* menu and select the *This server* menu item.

   The *Resources This Server Is Sharing With the Network* dialog box appears.

3. Highlight the sharename of the directory you want to stop sharing.

4. Select the *Delete* command button.

   The *Stop Sharing a Network Resource* dialog box appears, asking you to confirm your decision to stop sharing the resource. (Figure 7-5).

5. Select the *OK* command button.

   The directory is removed from the server's list of shared resources.

Example

You have been sharing a directory on the *mis.serve* server with a number of executives. This directory, which has been assigned the sharename *fiscal*, contains highly sensitive financial data. You are directed to move this information to the senior accountant's client, and to remove the shared directory from the network.

Before removing the directory from the *mis.serve* server, you must stop sharing it. First you start the Full Screen Net Admin Interface and access the server you wish to administer. From the *View* menu, you select the *This server* menu item. The *Resources This Server Is Sharing With the Network* dialog box appears. You highlight *fiscal* in the list box, then select the *Delete* command button. When the *Stop Sharing a Network Resource* dialog box appears, you check to make sure you are deleting the right directory before selecting the *OK* command button.

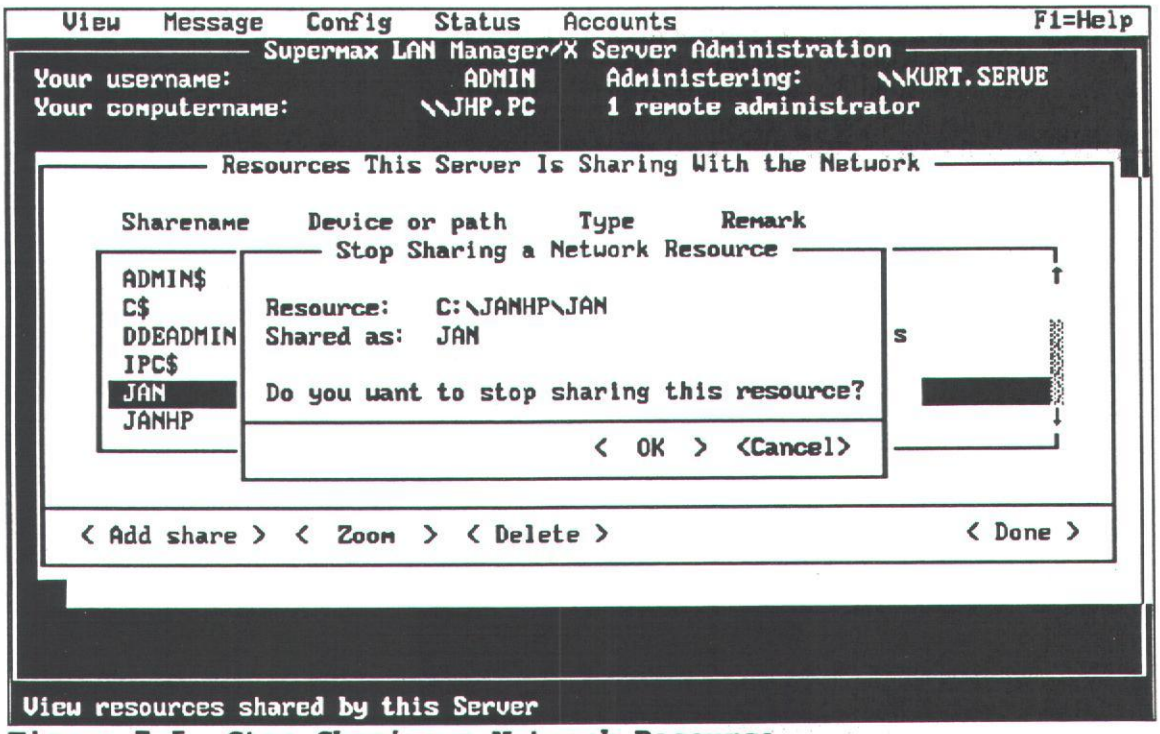


Figure 7-5. ***Stop Sharing a Network Resource***

7.5.1. Equivalent net Command

You can also unshare a directory with the **net share** command. For more information about the **net share** command, see Chapter 10, *Command Directory*.

7.6. Maintaining a Shared Disk

Because several people can create files in a shared directory, it is likely that a server's hard disk will fill up much more quickly than a client's hard disk. As administrator, you should closely monitor how much disk space is being used. The Server Program automatically tells you when a server's disk is near full-capacity. To conserve disk space, you should encourage users to take inventory of their files from time to time and to delete files they no longer need.

Finally, it is important to back up all shared directories on a regular basis. You should have a backup copy for each of the server hard disks in case anything happens to them. It is also helpful to back up copies of files you no longer want on the hard disk.

This section contains instructions for maintaining a shared disk, including information about managing server disk space, and backing up and restoring server files.

7.6.1. Managing Server Disk Space

To ensure efficient use of network resources, you should regularly check how much server disk space is available. If there is too little free disk space, you will want to make more available.

Caution: Do not use the root directory (/) to store files and directories created by the server. Otherwise, you may exhaust free disk space in the root file system and crash the server's UNIX system. For information about specifying the proper locations for shared directories, refer to the section entitled *Recommended Locations for Creating New Shared Directories*, in Chapter 4.

The UNIX operating system provides commands that allow you to evaluate per-user disk space consumption and total disk space consumption on the server. A summary description of these commands appears below. For complete information concerning the commands, see the documentation provided with your UNIX system.

To determine disk space consumption on a per-user basis, use the UNIX system **du** command. For example, to determine how much disk space determine how much disk space user *aaron* is currently using, at the UNIX system prompt type

```
du -s /usr/lanman/aaron
```

and press RETURN. The system displays information similar to the following:

```
6048 /usr/lanman/aaron
```

meaning that */usr/lanman/aaron* contains 6048 blocks of data.

To determine total disk space consumption, type

sysadm diskuse

and press RETURN. The system displays information similar to the following:

File System	Free Blocks	Total Blocks	Percent Full
/	3072	20088	84%
/usr	48918	149364	67%
/usr2	64432	114210	43%

7.6.2. Backing Up and Restoring Server Files

To back up and restore server files, you can select either of the following methods:

* Use the DOS **xcopy** command as described in your DOS user's guide.

* Use the System Administration Menu package, also known as *sysadm*. For more information on backing up and restoring server files using the System Administration Menu package, see *Supermax Basic Utilities, System V, Reference Manual. Section 1, Essential Utilities.*

Using the System Administration Menu package you can quickly back up all relevant files on your server. Using **xcopy**, you must work on a shared directory-by-shared directory basis.

In addition to user files and network applications, you should back up all files in the */usr/net/servers/lanman* and */usr/lanman* (or */usr2/lanman*) directories. These files contain information on the server's shared resources (shared printers, shared directories, and home directories). If these files are corrupted or lost and no backup is available, you will have to set up these resources again (by repeating the entire set up process).

8. Managing Shared Printers

8.1. Overview

As the administrator, you must decide which printers to share with network users and how to share them. When sharing printers, you must set up print queues and determine whether or not to create printer pools.

In addition to printers connected to the server, you can buy a special option which allows you to share printers connected to specially configured DOS clients. These printers are called *shared client printers*. Though shared printers can only be connected physically to DOS clients, they may be accessed by any client on the network, regardless of its operating system.

Using the information in this chapter, you can

* Understand how shared print queues work
* Understand the options for shared print queues
* Create a shared print queue
* Assign access permissions for printer resources
* Define customized print processor scripts
* Make shared print queues unavailable
* Change shared print queue options
* Change shared print queue status
* Pause and restart printer devices
* List and control print jobs

8.2. Understanding Shared Print Queues

Shared printers are printers that work with the Server Program and the UNIX system's *lp* subsystem (this subsystem contains the UNIX system's instructions for handling print jobs). A shared printer can be connected directly to either a Basic DOS or Enhanced DOS client on the LAN, provided you have obtained the *LAN Manager/X DOS Client Print*, or to the server (via serial or parallel port), or to a Network Terminal and Printer Controller (*NTC2*) connected to the server via its MIOC. The *lp* subsystem mediates between the Server Program and the printer, allowing print jobs to execute while users perform other tasks from their clients.



Users access shared printers by sending their print jobs over the network to the *shared print queues* that you create. A single shared print queue may contain one or many shared printers, or it may contain special programs known as *print processor scripts* that process the print job and send it on to a shared printer or other destination. Shared print queues are accessed over the network like any other shared resource.

This section contains information to help you understand shared printers, shared print queues, and print processor scripts.

8.2.1. How Do Shared Print Queues Work?

There are several ways that a print job can be routed to its final destination when a user sends it to a shared print queue:

* The shared print queue sends the print job directly to the UNIX system's *lp* subsystem. The *lp* subsystem then sends the print job to the printer or printers that are members of the shared print queue.

* The shared print queue sends the print job to a print processor script, which performs its pre-programmed actions on the print job. (You program the print processor script, and therefore control its function.) Next, the print processor script may send the print job to the UNIX system's *lp* subsystem (which will send it to one of the printers that are members of the shared print queue), or it may send the print job to some other destination (for example, it may send the print job output to another UNIX system).

The Server Program automatically sends messages similar to the following to notify users when their jobs are printed:

```
Your print job #9999 has finished printing on LASERQ.
```

The Server Program also notifies users if there are either problems with print jobs (if the printer is capable of such notification) or changes in the status of a print job (for instance, if an administrator pauses the queue).

8.2.2. Options for Shared Print Queues

The Server Program allows you either to create simple shared print queues that send print jobs to one printer, or to create more sophisticated shared print queues that send print jobs to a pool of printers. When setting up a shared print queue, you must consider these options:

* Which printers should receive print jobs from this shared print queue? (For more information, see *The Printer Devicename Option*, later in this section.)

* What priority level you want to assign to this shared print queue? (For more information, see *The Queue Priority Option*, later in this section.)

* At what times should the shared print queue service print jobs? (For more information, see *The Scheduling Option*, later in this section.)

* Do you want to use a print processor script to process print jobs sent to this shared print queue? (For more information, see *The Print Processor Option*, later in this section.)

* Do you want a separator page to be printed between print jobs for this queue, and, if you do, what will that page look like? (For more information, see *The Parameters Option* and *The Separator Page Option*, later in this section.)

The following sections describe these options and how they are associated with shared print queues.

8.2.2.1. The Printer Devicename Option

There are a number of ways you can configure print queues. In order of increasing complexity, you can configure:

* A single shared print queue associated with a single printer.

* Multiple shared print queues (each with different options) associated with a single printer.

* A single shared print queue associated with multiple printers of the same type.

Single Shared Print Queue Associated with a Single Printer

The simplest queue to create is one that sends print jobs to a single printer not associated with any other queue. To create such a queue, you must specify a sharename for the shared print queue and you must know the server devicename for the printer.

Note: Printer devicenames must conform to the naming conventions of the UNIX operating system. UNIX system printer devicenames may contain no more than 14 alphanumeric characters and the underscore (_).

Multiple Shared Print Queues Associated With a Single Printer

If you decide to assign two or more shared print queues (each having different options) to the same printer or group of printers, you may want to vary the users or groups who can access the various shared print queues, the priority levels of the shared print queues, and the times at which the different shared print queues can send print jobs to the printers.

You can specify the users or groups who can access a shared print queue either by editing the queue's access permissions (on a server running user-level security) or by controlling the resource's password (on a server running share-level security).

Single Shared Print Queue Associated With Multiple Printers
When you assign two or more printers of the same kind to a single shared print queue, you are creating a pool of printers. Using a shared print queue routed to a pool of printers is convenient for users. By using such a queue, the Server Program searches for an available printer automatically, and routes print jobs to the first available printer in the pool of printers associated with the shared print queue.

The Alerter service sends popup messages to users telling them the specific printer where their print jobs have been printed.

To create a print queue associated with two or more printers, you must define the sharename for the shared print queue and the devicenames for all printers in the pool.

8.2.2.2. The Queue Priority Option

Administrators can assign priority levels to shared print queues. (The highest priority is 1, the lowest is 9, and the default is 5.) If you find that certain print requests are more time critical than others, you can create two shared print queues for the same printer or printer pool. For example, you could create one shared print queue named *high* with a priority of 1 and another shared print queue named *average* with a priority of 5. Requests in the *high* shared print queue would be printed before requests in the *average* shared print queue. Then you could give access permissions for the *average* shared print queue to all users, and for *high* only to users who need to print time-critical documents.

8.2.2.3. The Scheduling Option

The scheduling option lets you specify the times at which a shared print queue can send print jobs to the printers. Users can submit print jobs to the shared print queue at any time, but the shared print queue holds all requests until its designated start-printing time.

8.2.2.4. The Print Processor Option

Use the print processor option to specify the filename of a print processor script for use by the shared print queue. *Print processor scripts* contain programs for manipulating print jobs. Instead of sending the print job directly to the UNIX system's *lp* subsystem, the shared print queue sends it to the print processor script you specify with the print processor option. (When specifying this option, you need only provide the name of the file containing the print processor script; all print processor scripts are stored in the */usr/net/servers/lanman/customs* directory.)

After processing the print job, the print processor script can use a UNIX system pipe to redirect the print job to the *lp* subsystem.

The file containing the print processor script must be a UNIX system executable file. Usually, it is created using a text editor. For more information about print processor scripts, see the section entitled *Defining Customized Print Processor Scripts*, p.8-13).



8.2.2.5. The Parameters Option

The Server Program supports the following parameters for print queues:

COPIES - specifies how many copies of a print job should be printed. Specify a number.

TYPES - specifies the content type (also known as the file type) of the files that will be sent to the printer queue.

EJECT - specifies whether or not a page feed should occur between copies for a multiple-copy print job. Specify `auto` (default) or *yes* if you want page feeds between copies. Otherwise, specify *no*.

BANNER - specifies whether or not to print a separator page (banner) between print jobs. Specify `yes` or `no`.

8.2.2.6. The Separator Page Option

The Server Program automatically prints out a banner or separator page before each print job. You may select to alter the default banner or separator page and create one more suitable to your needs. In the field, specify the name of the file containing your banner page. This file should be an ASCII text file, containing what-you-see-is-what-you-get text.

The default directory for storing *separator page*-files is */usr/net/servers/lanman/spool*.

8.3. Creating Shared Print Queues

Once you have a basic understanding of how shared printers work on the LAN, you can begin to perform the tasks required to set up and maintain printer services on the LAN. This section provides instructions for performing the following tasks:

* Creating a shared print queue by using the Full Screen Net Admin Interface
* Assigning access permissions for printer resources
* Defining customized print processor scripts
* Making shared print queues unavailable

8.3.1. Creating a Shared Print Queue by Using the Full Screen Net Admin Interface

Once you have decided how to set up your shared print queues, you can begin to create them on the server.

Note: Before you can successfully create a shared print queue on the server, the UNIX system must be configured for each printer associated with the shared print queue. For more information and the procedure to configure the UNIX system for printers connected to the server, see Chapter 7, *LP Spooler Administration* in the *Supermax System V, System Administrator's Guide.*

To create a shared print queue by using the Full Screen Net Admin Interface, follow these steps:

1. Start the Full Screen Net Admin Interface and access the server on which you want to share a printer. (For instructions, see the section entitled *Accessing the Full Screen Net Admin Interface*, in Chapter 3).

2. Select the *View* menu and select the *This server* menu item.

   The *Resources This Server Is Sharing With the Network* dialog box appears.

3. Select the *Add Share* command button.

   The *What would you like to share?* dialog box appears.

4. Select the *Spooled printer* option button and then select the *OK* command button.

   The *Share a Print Queue With the Network* dialog box appears. (Figure 8-1).

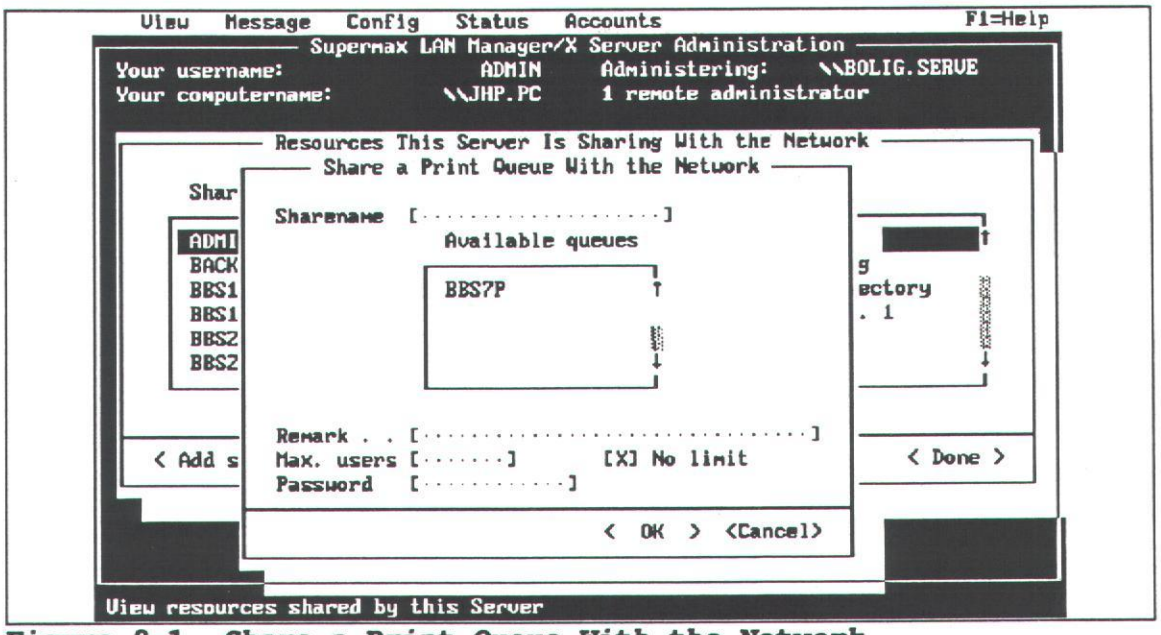


Figure 8-1. *Share a Print Queue With the Network*

5. Enter information into the text boxes of the *Share a Print Queue With the Network* dialog box as follows.

   a) At the *Sharename* text box, type the sharename you want the shared print queue to have. Do not enter a name that is already being used by any of the server's UNIX system *lp* devicenames (printer names). If you share multiple print queues on the server, each of their sharenames must be unique. Sharenames for shared print queues can have up to 8 alphanumeric characters.

   b) At the *Remark* text box, type a comment describing the shared print queue.

   c) At the *Max. users* text box, type the maximum number of users that will be able to use this queue at any one time. If you do not wish to set a maximum number of users, mark the *No limit* check box.

   d) The *Password* text box is not used on servers running user-level security. On servers running share-level security, at the *Password* text box, enter a password for the shared print queue to prevent unauthorized use. On servers running share-level security, passwords can have a maximum of 8 alphanumeric characters.

6. Select the *OK* command button.

   One of the following occurs:

   * If the shared print queue does not already exist, a message box displays this message:

     ```
     The specified printer queue does not exist.
     Click <OK> to create the queue <sharename>.
     ```

     where *<sharename>* is the name you have chosen for the shared print queue. Proceed to Step 7.

   * If the shared print queue already exists, the system displays an error message. Select the *OK* command button. The system displays the *Resources This Server Is Sharing With the Network* dialog box. Choose a new name for the shared print queue and return to Step 3.

7. Select the *OK* command button to create the shared print queue.

   The *Printing Options for Queue* dialog box appears. (Figure 8-2).

8. Enter information into the text boxes of this dialog box as follows:

   a) At the *Priority* text box, set the priority for this queue by typing a number between 1 and 9. (1 is the highest priority, 9 is the lowest, and 5 is the default setting.)

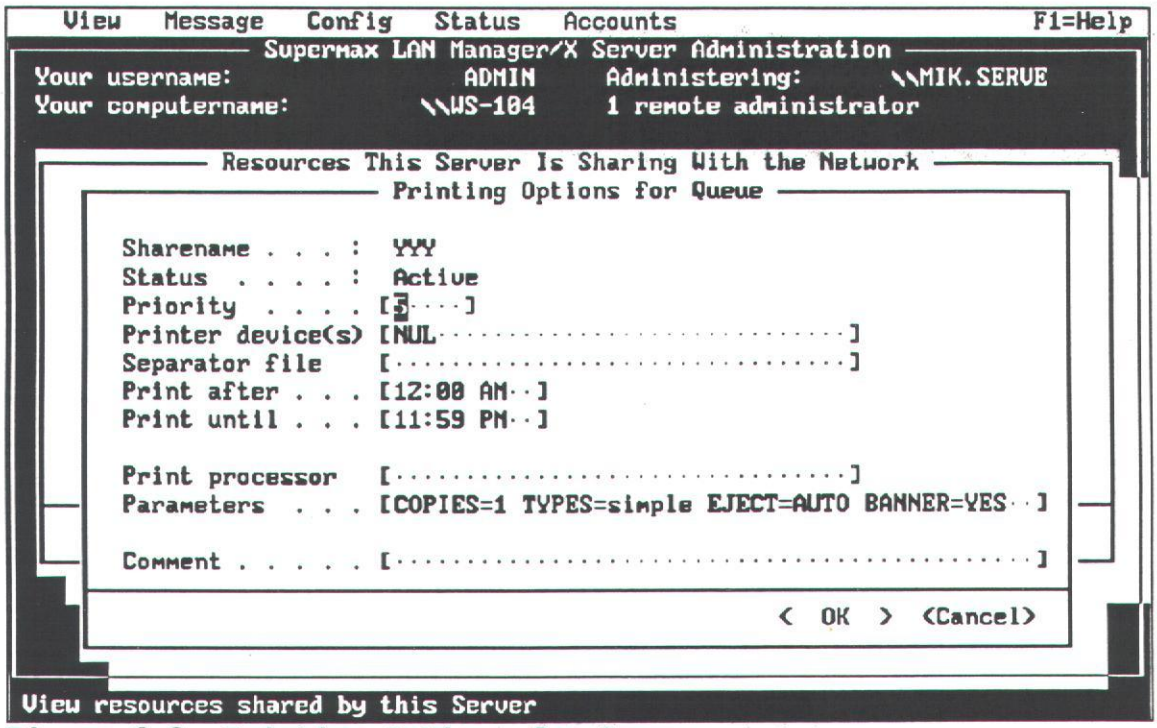


Figure 8-2. *Printing Options for Queue*

b) At the *Printer device(s)* text box, type the UNIX system *lp* printer names for the printer(s) to be included in the LAN Manager queue. The printers specified here will be the printers that actually print jobs submitted to this shared printer queue.

If the shared print queue will route print jobs to a pool of printers, separate the devicenames with spaces. For example,

```
laser1 laser2
```

Leave this text box set to *NUL* if this queue will use a print processor script.

c) At the *Separator file* text box, type the pathname of the separator file you want to use with this queue, if any. This can be a relative pathname or an absolute pathname. Relative pathnames are assumed to begin in the */usr/net/servers/lanman/spool* directory; absolute pathnames are assumed to begin at the server's root (/) directory. If you want to use the default banner page, leave this field blank.

d) At the *Print after* text box, type the time at which the shared print queue can start sending requests to the printer(s). Use *either* 24-hour format (00:00 - 23:59) or 12-hour format (12:00 AM - 11:59 PM). The printer will begin printing within ten minutes of the time you specify.

e) At the *Print until* text box, type the time after which the shared print queue can no longer send requests to the printer(s). Use *either* 24-hour format (00:00 - 23:59) or 12-hour format (12:00 AM - 11:59 PM). The printer will stop printing within ten minutes of the time you specify.

f) At the *Print processor* text box, type the name of the customized print processor script file to be used with this queue, if any. Enter only the filename (a full pathname is not required, as all print processor script files are stored in the server's */usr/net/servers/lanman/customs* directory).

A print processor script can be used to perform customized processing of jobs submitted to a shared print queue.

g) At the *Parameters* text box, type any parameters for the queue. The Server Program supports the following parameters:

COPIES - specifies how many copies of a print job should be printed. Specify a number.

TYPES - specifies the content type (also known as the file type) of the files that will be sent to the queue by default. The content type accepted by a queue is determined by the content type accepted by the first printer specified in the queue. Therefore, once you complete the *Printer Device(s)* text box in Step (b and press RETURN, the *TYPES* field will automatically contain the content type for the first printer specified in the text box.

Note: Normally, you will not need to change the value in the *TYPES* field from the value that automatically is assigned to it. However, if you are sending ASCII files to a printer queue which contains PostScript printers, the *TYPES* field should be set to `simple`. If you do not set this field to `simple`, the job will not print (although you will receive a message that the job has printed). For more information about content types, see the section on configuring printers in the *Supermax System V, System Administrator's Guide*.

EJECT - specifies whether or not a page feed should occur at the end of every completed print job. Specify `yes` or `no`.

BANNER - specifies whether or not to print a separator page (banner) between print jobs. Specify `yes` or `no`.

h) At the *Comment* text box, type a comment describing the shared print queue.

9. Select the *OK* command button.

* If the server is running share-level security, the *Resources This Server Is Sharing With the Network* dialog box appears. You have completed this procedure.



* If the server is running user-level security, the *Add Permissions* dialog box appears. Proceed to Step 10.

10. Determine how you want to specify access permissions for the queue:

    * If you want to use the default access permissions, select the *Use default permissions* option button. This will assign the *Yes* access permission to the default set of users and groups (configured with the *\PRINT* special printer resource). Proceed to Step 11.

    * If you want to specify access permissions for the queue on an individual user and group basis, select the *Set explicit permissions* option button.

      Use the two list boxes, the access permission option buttons, and the *Move* command button to specify the access permissions for each user and group as follows:

      * To add a user or group to the *Permitted* list box, highlight that username or groupname in the *Not permitted* list box, select the *Yes* access permission option button, and select the *Move* command button. The user or group moves to the *Permitted* list box, with the *Yes* access permission assigned. Each resource can have up to 64 entries in the *Permitted* list box.

        Note: If the access permission option button is set to *No* when you move a username into the *Permitted* list box, then you are preventing that user from using the resource. This occurs regardless of the groups to which that user belongs.

      * To remove a user or group from the *Permitted* list box, highlight that username or groupname and select the *Move* command button.

      * To change the access permissions for a user or group in the *Permissions* list box, highlight that username or groupname and select one of the access permission option buttons.

11. If you want to record who uses this queue, when it is used, and what is done with the queue, mark the *Audit this resource* check box. To use this feature, the Audit Trail must be enabled on this server (using the *auditing=* parameter in the *[server]* section of the server's *lanman.ini* file). To set the value of this parameter, see Chapter 9, *Changing the Default Server Configuration*.

12. Select the *OK* button.

Example
You are setting up two printers to be accessed on the *print1.serve* server. You decide to create a single shared print queue for the two printers.

Using the Full Screen Net Admin Interface, you access the *print1.serve* server. You select the *View* menu and select the *This server* menu item. Then, in the *Resources This Server Is Sharing With the Network* dialog box, you select the *Add share* command button. In the *What would you like to share?* dialog box, you select the *Spooled printer* option button and then select the *OK* command button. In the *Share a Print Queue With the Network* dialog box you type the sharename of the shared print queue you want to create (*pool1*), and then a descriptive remark for it. Because the *print1* server runs share-level security, you also type in a password for the print queue before selecting the *OK* command button.

The *Printing Options for Queue* dialog box appears. You type the devicenames for both printers in the *Devicename* text box:

```
laser1 laser2
```

You also type in the name of the separator file that is to print between each document, and a comment that you will see if you decide to change the print options later. When you select the *OK* command button, the new *pool1* queue appears in the list of shared resources for the *print1* server.

8.3.1.1. Equivalent net Command

You can also create a shared print queue using the **net share** command. After creating the shared print queue, you can reconfigure its options using the **net print** command. For more information about the **net share** and the **net print** commands, see Chapter 10, *Command Directory*.

8.3.2. Assigning Access Permissions for Printer Resources

To look at or change access permissions for a shared print queue, you must supply the *\print\sharename* for the shared print queue in question.

For all shared print queues, LAN Manager maintains a default set of access permissions. You can change the default access permissions by changing access permissions on the special printer resource sharename *\print*.

You can create shared print queues automatically by sharing a queue that does not yet exist. When you do this, LAN Manager prompts you for access permissions for the new queue.

You may need to change access permissions under the following circumstances:

* You want to stop using default access permissions for the shared print queue.

* You want to assign, change, or delete access permissions for a user or group.

Procedure

To change access permissions for a shared print queue, follow these steps:

1. Start the Full Screen Net Admin Interface and access the server you wish to administer. (For instructions, see the section entitled *Accessing the Full Screen Net Admin Interface*, in Chapter 3.)

2. Select the *Accounts* menu and select the *Other permissions* menu item.

   The *Other Access Permissions* dialog box appears.

3. In the list box, highlight the resource whose access permissions you want to change and then select the *Change* command button.

   The *Change Permissions* dialog box appears.

4. Select the *Set explicit permissions* option button.

   The *\print* resource must always have explicit access permissions, since it represents the default for other printer resources.

5. Mark the *Audit this resource* check box if you want to record who uses this queue, when it is used, and what is done with the queue. To use this feature, the Audit Trail must be enabled on this server (using the *auditing=* parameter in the *[server]* section of the server's *lanman.ini* file). To set the value of this parameter, see Chapter 9, *Changing the Default Server Configuration*.

6. Use the two list boxes, the access permission option buttons, and the *Move* command button to specify the access permissions for each user and group as follows:

   * To *add* a user or group to the *Permitted* list box, highlight that username or groupname in the *Not permitted* list box and select the *Move* command button. The user or group moves to the *Permitted* list box. Each resource can have up to 64 entries in the *Permitted* list box.

     Note: If the access permission option button is set to *No* when you move a username into the *Permitted* list box, then you are stipulating that the user in question cannot use the resource, regardless of the groups to which that individual may belong.

   * To *remove* a user or group from the *Permitted* list box, highlight that username or groupname and select the *Move* command button. The user or group moves to the *Not permitted* list box.

   * To *change* access permissions for a user or group in the *Permitted* list box, highlight that username or groupname and select one of the access permission option buttons.

7. Select the *OK* command button.

   The *Other Access Permissions* dialog box appears.

8. Select the *Done* command button to return to the background screen.

8.3.3. Defining Customized Print Processor Scripts

By default, the Server Program sends all print jobs to the *lp* subsystem of the UNIX system, which queues and prints them using the UNIX system **lp** command. However, you can define customized print processor scripts.

You can define customized print processor scripts that will send print jobs directly to a file or a terminal, send print jobs to remote computers with the UNIX system **uucp** command, or format text with the UNIX system **troff** or **nroff** commands.

After you define a customized print processor script, you must share it to allow users to access it. (For instructions, see the section of this chapter entitled *Creating A Shared Print Queue by Using the Full Screen Net Admin Interface*, p.8-5).

To access the script, users link to the sharename as they would link to a shared print queue, and then use a print command (for example, the DOS **copy** command) and specify the file to be printed. You can define an unlimited number of customized print processor scripts.

This section contains the following information:

* Guidelines to use when defining scripts
* Environmental variables that can be included in scripts
* Sample scripts
* How to define a script by using a text editor

After you have defined a print processor script, inform users of the existence of the script, its use and functionality and its sharename.

8.3.3.1. Guidelines to Use When Defining Scripts

A print processor script is a program conforming to the guidelines listed in this section; it is made up of UNIX system shell commands, some special environmental variables, and some special statements.

To avoid affecting service to other users, execute scripts in the background. If a script is run in the background, the file to be printed should first be copied to a temporary file. This temporary file should be used by the rest of the script. For example, the following command could precede a script:

```
/bin/cp $FILENAME /tmp/myfile$$
```



8.3.3.2. Environmental Variables that Can Be Included in Scripts

You can include the following environmental variables in print processor scripts:

* **$CLIENT** - the computername from which the print job was sent.

* **$COPIES** - the number of copies (1-99) to be printed.

* **$PRIO** - the UNIX system **lp** priority (1-39) of the print job.

* **$DEST** - the UNIX system **lp** printer class (server queue) to which the job will be sent.

* **$FILENAME** - the full pathname of the file to print.

8.3.3.3. Sample Scripts

The following are two sample customized printer scripts.

The first print processor script formats and displays a file on the console:

```
/bin/cp $FILENAME /tmp/myfile$$
(
/bin/pr -n:3 -h "$FILENAME from $CLIENT "\
-115 /tmp/myfile$$> /dev/console
/bin/rm /tmp/myfile$$
)&
```

The second print processor script sends a file to a user on a remote system:

```
/bin/cp $FILENAME /tmp/myfile$$
(
/usr/bin/uuto /tmp/myfile$$ system!user
/bin/rm /tmp/myfile$$
)&
```

Replace *system* with the name of the system the user is on; replace *user* with the name of the user.

8.3.3.4. Defining Scripts by Using a Text Editor

You should perform this procedure only if you are an experienced UNIX system administrator and are familiar with writing scripts for the UNIX system shell.

To define a customized print processor script by using a text editor, follow these steps:

1. Use a text editor (such as *vi*) to create a file that contains your print processor script. Save that file in the server's */usr/net/servers/lanman/customs* directory.

Note: The filename must be a legal DOS filename, i.e. containing up to 8 alphanumeric characters with an extension containing up to 3 characters. Your print processor script file must contain ASCII text. In order to run, it must have UNIX execute permission.

2. Create the shared print queue for which you are writing the printer script using the instructions from the section of this chapter entitled, *Creating Shared Print Queues*. When entering information in the *Printing Options for Queue* dialog box, type the name of the file containing the print processor script file in the *Print processor* text box.

8.3.4. Making Shared Print Queues Unavailable

You may want to stop sharing a shared print queue at some point. For example, you may be reorganizing your shared print queues, removing a printer (this only affects the shared print queue if this printer is the only printer in the queue), or perhaps a particular shared print queue has simply become unnecessary.

8.3.4.1. Unsharing Shared Print Queues by Using the Full Screen Net Admin Interface

If you are at either an Enhanced DOS or OS/2 client, you can unshare a shared print queue by using the Full Screen Net Admin Interface. To do so, follow these steps:

1. Start the Full Screen Net Admin Interface and access the server you wish to administer. (For instructions, see the section entitled *Accessing the Full Screen Net Admin Interface*, in Chapter 3.)

2. Select the *View* menu and select the *This server* menu item.

3. In the *Resources This Server Is Sharing With the Network* dialog box, select the name of the shared print queue you want to stop sharing and then select the *Delete* command button.

   The *Stop Sharing a Network Resource* dialog box appears, asking you to confirm your decision to stop sharing the printer.

4. Select the *OK* command button.

   The print queue still exists (it can be displayed using the **net print** command), but it is unavailable to network users. To completely delete the print queue from the server, see the section of this chapter entitled, *Changing Shared Print Queue Status*, p.8-19.

Example

You are reorganizing the server's shared print queues and decide that the *laser2* shared print queue is no longer needed.

To stop sharing the printer, you invoke the Full Screen Net Admin Interface and access the server you wish to administer.

From the *View* menu, you select the *This server* menu item. In the *Resources This Server Is Sharing With the Network* dialog box, you highlight the *laser2* shared print queue and select the *Delete* command button to stop sharing the shared print queue.

8.3.4.2. Equivalent net Command

You can also stop sharing a shared print queue using the **net share** command. For more information about the **net share** command, see Chapter 10, *Command Directory*.

8.4. Managing Shared Print Queues and Print Jobs

This section describes how to manage shared print queues and print jobs. It contains instructions for performing the following tasks:

* Changing shared print queue options
* Changing shared print queue status
* Controlling printers by sharename
* Listing and controlling print jobs

8.4.1. Changing Shared Print Queue Options

The Server Program allows you to change the options for an existing shared print queue. For example, you may want to add another printer to the queue or revise the queue's description. From a client running the Full Screen Net Admin Interface, you can change the options for an existing shared print queue.

From an Enhanced DOS or OS/2 client, you can change the options for a shared print queue by using the Full Screen Net Admin Interface. To do this, follow these steps:

1. Start the Full Screen Net Admin Interface and access the server you wish to administer. (For instructions, see the section entitled *Accessing the Full Screen Net Admin Interface*, in Chapter 3.)

2. Select the *View* menu and select the *Print queues* menu item.

   The *Show Print Queues For...* dialog box appears.

3. Identify the shared print queue(s) you want to examine by doing *one* of the following:

   * Type the name of the server sharing the queue in the *Server* text box.
   * Select the server from the *Visible servers* list box.

* Select the local devicename that is connected to the queue from the *Redirected devices* list box.

4. Select the *Zoom* command button.

   The *Print Queues for (server)* dialog box appears.

5. Select the sharename of the shared print queue you want to change.

6. Select the *Zoom* command button.
   The *Printing Options for Queue* dialog box appears, showing the current options for this shared print queue.

7. Enter information into the text boxes of this dialog box as follows:

   a) At the *Priority* text box, set the priority for this queue by typing a number between 1 and 9. (1 is the highest priority, 9 is the lowest, and 5 is the default setting.)

   b) At the *Printer device(s)* text box, type the UNIX system *lp* printernames for the printer(s) to be included in the queue. The printers specified here will be the printers that actually print jobs submitted to this shared print queue.

      If the shared print queue will route print jobs to a pool of *lp* printers, separate the *lp* printernames with spaces. For example,

      ```
      laser1 laser2
      ```

      Leave this text box set to *NUL* if this queue will use a print processor script.

   c) At the *Separator file* text box, type the pathname of the separator file you want to use with this queue, if any. This can be a relative pathname or an absolute pathname. Relative pathnames are assumed to begin in the */usr/net/servers/-lanman/spool* directory; absolute pathnames are assumed to begin at the server's root (/) directory. If you want to use the default banner page, leave this field blank.

   d) At the *Print after* text box, type the time at which the shared print queue can start sending requests to the printer(s). Use *either* 24-hour format (00:00 - 23:59) or 12-hour format (12:00 AM - 11:59 PM). The printer will begin printing within ten minutes of the time you specify.

   e) At the *Print until* text box, type the time after which the shared print queue can no longer send requests to the printer(s). Use *either* 24-hour format (00:00 - 23:59) or 12-hour format (12:00 AM - 11:59 PM). The printer will stop printing within ten minutes of the time you specify.

f) At the *Print processor* text box, type the name of the customized print processor script file to be used with this queue, if any. Enter only the filename (a full pathname is not required, as all print processor script files are stored in the same directory).

A print processor script can be used to perform customized processing of jobs submitted to a shared print queue.

g) At the *Parameters* text box, type any parameters for the queue. The Server Program supports the following parameters:

COPIES - specifies how many copies of a print job should be printed. Specify a number.

TYPES - specifies the content type (also known as the file type) of the files that will be sent to the queue by default. The content type accepted by a queue is determined by the content type accepted by the first printer specified in the queue. Therefore, once you complete the *Printer Device(s)* text box in Step (b and press RETURN, the *TYPES* field will automatically contain the content type for the first printer specified in the text box.

Note: Normally, you will not need to change the value in the *TYPES* field from the value that automatically is assigned to it. However, if you are sending ASCII files to a printer queue which contains PostScript printers, the *TYPES* field should be set to `simple`. If you do not set this field to `simple`, the job will not print (although you will receive a message that the job has printed). For more information about content types, see the section on configuring printers in the *Supermax System V, System Administrator's Guide*.

EJECT - specifies whether or not a page feed should occur between copies for a multiple-copy print job. Specify `auto` (default) or `yes` if you want page feeds between copies. Otherwise, specify `no`.

BANNER - specifies whether or not to print a separator page (banner) between print jobs. Specify `yes` or `no`.

h) At the *Comment* text box, type a comment describing the shared print queue.

8. Select the *OK* command button.

Example
You have just created a new separator file to use with the *pool1* shared print queue. Now you need to add the name of the new separator file to the shared print queue options. First, you invoke the Full Screen Net Admin Interface and access the server you wish to administer. From the *View* menu, you select the *Print queues* menu item. In the *Show Print Queues For...* list box you highlight the *print1.serve* server and then select the *Zoom* command button. In the *Print Queues for \\PRINT1.SERVE* list box you highlight the *pool1* shared print queue and then select the *Zoom* command button.

When the *Printing Options for Queue* dialog box appears, you move to the *Separator* file text box, type the full pathname of the new separator file, and select the *OK* command button.

The next time someone prints a print job using the *pool1* queue, the new separator page is automatically printed before their print job.

8.4.1.1. Equivalent net Command

You can also change the options for existing shared print queues by using the **net print** command. For more information about the **net print** command, see the Chapter 10, *Command Directory*.

8.4.2. Changing Shared Print Queue Status

Just as you can change the status of print jobs in a shared print queue, you can change the status of the queue itself. You may change the status of the shared print queue to perform any of the following functions:

* Hold a shared print queue so that all print jobs after the one currently being printed are held. These print jobs do not print until the shared printer queue is released from the hold.

  Note: You cannot hold print jobs sent to a shared print queue that uses a print processor script. Even if the status of the shared print queue is changed to *hold,* the print job will be processed.

* Release a shared print queue from hold.

* Delete a shared print queue.

* Purge a shared print queue of all print jobs.

These tasks can only be performed by using the Full Screen Net Admin Interface.

To change the status of a shared print queue, follow these steps:

Note: To change the status of a shared print queue, you must be logged in as *admin* or as a user with administrative privileges.

1. Start the Full Screen Net Admin Interface and access the server you wish to administer. (For instructions, see the section entitled *Accessing the Full Screen Net Admin Interface*, in Chapter 3.)

2. Select the *View* menu and select the *Print queues* menu item.

   The *Show Print Queues For...* dialog box appears.

3. Identify the server whose shared print queue you want to change by doing *one* of the following:

   * Type the name of the server sharing the queue in the Server text box.

   * Highlight the server in the *Visible servers* list box.

   * Highlight the local devicename that is connected to the queue in the *Redirected devices* list box.

4. Select the *Zoom* command button.

   The *Print Queues for <server>* dialog box appears, where *<server>* is the name of the server you identified in Step 3.

5. Highlight the sharename of the shared print queue whose status you want to change.

6. Select *one* of the following command buttons:

   * *Hold* - to hold all print jobs (except the one that is currently being printed) in the queue.

     Note: You cannot hold print jobs sent to a shared print queue that uses a print processor script. Even if the status of the shared print queue is changed to *hold* the print job will be processed.

   * *Release* - to reactivate a held shared print queue.

     Note: Releasing a shared print queue that is in an error condition will clear the error.

   * *Zoom* - to display the *Printing Options for Queue* dialog box. For more information, see the section entitled *Changing Shared Print Queue Options*, earlier in this chapter.

   * *Delete* - to delete a shared print queue once it is empty.

   * *Purge* - to remove all print jobs from the shared print queue without deleting the queue itself.

     Note: If the queue is currently pending delete, this will also delete the queue.

7. Select the *Done* command button to return to the *Show Print Queues For...* dialog box.

8. Select the *Done* command button again to return to the background screen.

Example
You need to use a printer connected to the *print2.serve* server; this printer is accessed using the *lineprt* shared print queue. Because the job you are sending to this printer is quite large, you decide to walk down to the printer and load it with paper. Before you go, you decide to hold the *lineprt* shared print queue, which is the only queue containing this particular printer. (If more than one print queue contained the printer, you could save time by pausing the printer device directly, using the instructions in the section of this chapter entitled *Controlling Printers by Sharename.*)

You start the Full Screen Net Admin Interface and access the *print2.serve* server.

You select the *View* menu and then select the *Print queues* menu item. In the *Show Print Queues For...* dialog box you highlight the *print2.serve* server and then select the *Zoom* command button. In the *Print Queues for \\PRINT2.SERVE* dialog box, you highlight the *lineprt* shared print queue and select the *Hold* command button.

When you are finished loading the printer, you can release the queue by highlighting the *lineprt* shared print queue and selecting the *Release* command button in the *Print Queues for \\PRINT2.SERVE* dialog box.

8.4.2.1. Equivalent net Command
You can also hold shared print queues using the **net print** command. For more information about the **net print** command, see Chapter 10, *Command Directory*.

8.4.3. Controlling Printers by Sharename
This section provides instructions for controlling printers (and affecting the print jobs that are running on them) by sharename. Using the instructions in this section, you can either pause/continue a specific printer or restart/kill the print jobs that are running on the printer.

To control printers by using the names of shared print queues, follow these steps:

1. Start the Full Screen Net Admin Interface and access the server you wish to administer. (For instructions, see the section entitled *Accessing the Full Screen Net Admin Interface*, in Chapter 3.)

2. From the *Status* menu, select the *Device status* menu item.

   The *Shared Device Status* dialog box appears. (Figure 8-3).

3. Highlight the desired printer in the list box.

4. Do *one* of the following:

   * To temporarily stop the printer's operation, select the *Pause* command button. The printer will stop running print jobs.

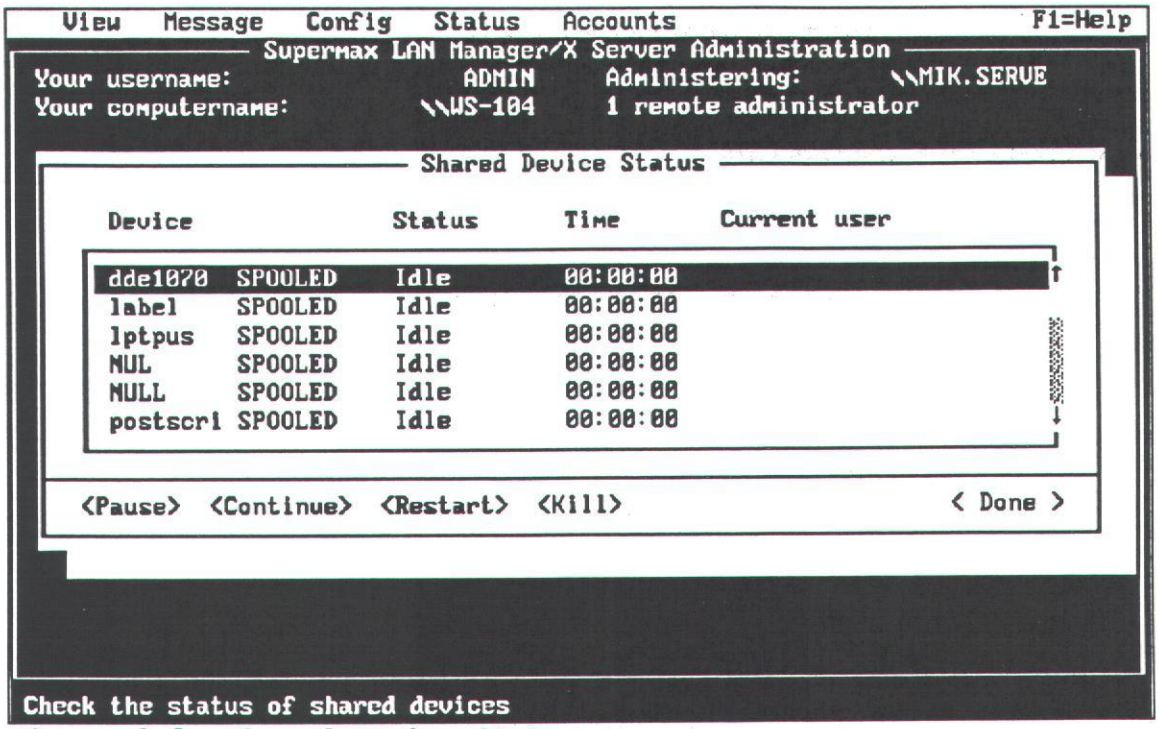


Figure 8-3. *Shared Device Status*

Any print job currently running on the printer will be re-queued, and will be reprinted completely by the next available printer. (If there is more than one printer associated with the shared print queue, another printer may run the print job.)

Note: You can only pause printers if the word *SPOOLED* appears next to the devicename in the list box.

* To cause a paused printer to continue printing, select the *Continue* command button. The printer will now run print jobs. Any print jobs that were interrupted when the printer was paused will be reprinted completely (provided that they have not already been printed by another printer in the shared print queue).

* To restart a print job currently running on the printer, select the *Restart* command button. The print job will stop, and then will be reprinted completely.

* To remove a print job currently running on the printer, select the *Kill* command button. The print job will be stopped and deleted from the shared print queue.

The new status for the printer is displayed in the list box.

5. Select the *Done* command button to return to the background screen.

8.4.3.1. Equivalent net Command

You can pause individual printers using the **net pause** command. You can restart individual printers using the **net continue** command. For more information about the **net pause** and **net continue** commands, see Chapter 10, *Command Directory*.

8.4.4. Listing and Controlling Print Jobs

Listing the print jobs for a shared print queue lets you monitor the status of individual print jobs. It also lets you perform the following tasks:

* Delete a print job
* Change the position of print job to the front or rear of a shared print queue
* Restart a print job that was interrupted while printing
* Hold a print job in a shared print queue so that it does not print
* Release a held print job so that it can be printed

To list and control print jobs for a shared print queue, follow these steps:

Note: Remember, in order to modify all print jobs, you must be logged in as *admin* or as a user with administrative privileges. If you do not have administrative privileges, you may modify only your own print jobs.

1. Start the Full Screen Net Admin Interface and access the server you wish to administer. (For instructions, see the section entitled *Accessing the Full Screen Net Admin Interface*, in Chapter 3.)

2. Select the *View* menu and select the *Print queues* menu item.

   The *Show Print Queues For...* dialog box appears. (Figure 8-4).

3. Identify the server whose shared print queues you want to examine by doing *one* of the following:

   * Type the name of the server sharing the queue in the *Server* text box.
   * Highlight the server in the *Server* list box.
   * Highlight the local devicename that is connected to the queue in the *Redirected device* list box.

4. Select the *Zoom* command button.

   The *Print Queues for* dialog box appears. (Figure 8-5).

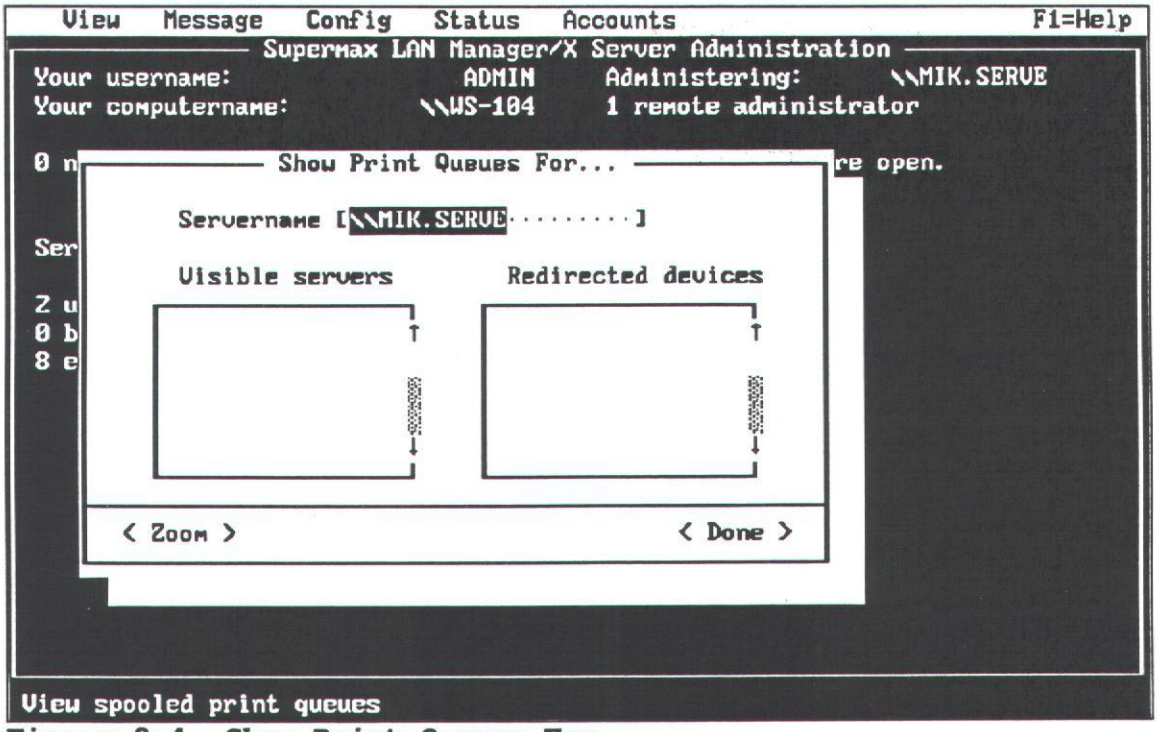


Figure 8-4. ***Show Print Queues For***

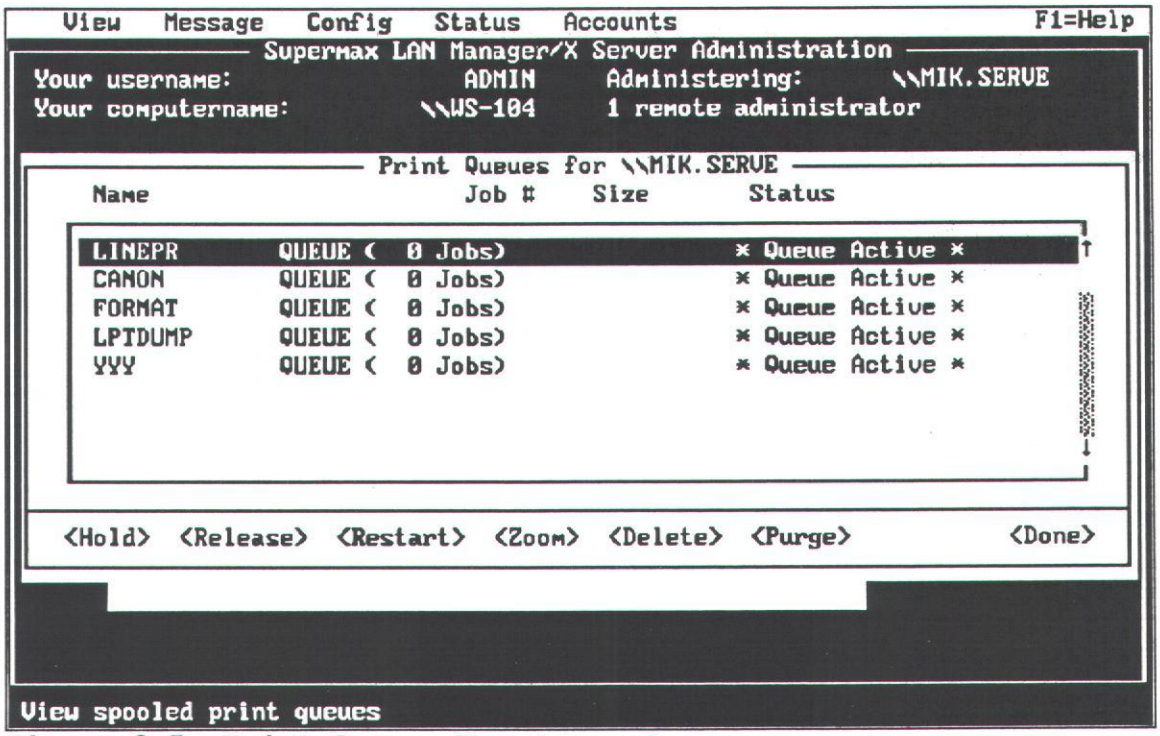


Figure 8-5. ***Print Queues For <server>***

The list box in this dialog box shows the sharename and status of each shared print queue shared from the server you selected in Step 3. It also shows the print jobs in the individual queues. The print jobs are indented slightly, and have a username in the left column, rather than a sharename.

5. Highlight the print job you want to modify.

6. Do *one* of the following:

   * To hold a print job in the queue without printing it, select the *Hold* command button.

   * To release a held print job so the it can be printed, select the *Release* command button.

   * To restart a print job that has stopped because of a printer error or for some other reason, select the *Restart* command button. The print job is reprinted from the beginning.

   * To move the print job to the front or back of the queue, or to see specific information about the print job, select the *Zoom* command button. When moving a print job in the shared printer queue, be aware of the following considerations:

     - If either the shared print queue or the print job itself is paused or held, you cannot move the print job.

     - If a print job is moved to the last place in the shared print queue, it receives a new job number. After the move, do not search mistakenly for the old job number.

     - If multiple print jobs are moved to the first place in the queue, you cannot reliably predict which will be the first to print. The system makes this decision on an arbitrary basis.

   * To remove a job from the shared print queue, select the *Delete* command button.

7. Select the *Done* command button to return to the background screen.

Example
You hear that there's something wrong with the *pool1* shared print queue on the *print1.serve* server. In response, you start the Full Screen Net Admin Interface and access the *print1.serve* server.

You select the *View* menu and select the *Print queues* menu item. You highlight the *print1.serve* server in the *Show Print Queues For...* list box and then select the *Zoom* command button.

The *Print Queues for* dialog box appears, showing that several print jobs are waiting in the queue. You walk to the printer room and discover that the printers are out of paper. When you return to your office, you send mail to the users who had print jobs waiting, to let them know the printers are working again.

8.4.4.1. Equivalent net Command

You can list the contents of a shared print queue by using the **net print** command. You can list the status of a particular printer by using the **net device** command. For more information concerning the **net print** and **net device** commands, see Chapter 10, *Command Directory*.

9. Changing the Default Server Configuration

9.1. Overview

The Server Program's configuration is determined by the values of the parameters stored in the server's *lanman.ini* file.

This chapter contains the following information about the server's configuration and the *lanman.ini* file:

* An explanation of how parameters affect the server program's operation.
* The conventions and organization used in the *lanman.ini* file.
* A list of the reconfigurable parameters found in the *lanman.ini* file, with a definition for each parameter.
* Instructions for changing the values of the parameters in the *lanman.ini* file and thereby reconfiguring the server using either a text editor or the UNIX program *srvconfig*.

9.2. Understanding How the Server Is Configured

The operation of the Server Program is influenced by a variety of *parameters* which define how the server works and how it can be used. The values of these parameters specify the names of computers, users, and programs, as well as information on resources, such as the amount of memory available to the Server Program.

When the Server Program is installed, default values are assigned to these parameters. You can reconfigure the Server Program by changing the values associated with each of its parameters. To do this, you must either use a text editor (such as *vi*) or the UNIX program *.srvconfig*.

All configurable Server Program parameters are contained in a file on the server called the *lanman.ini* file. This file is located in the */usr/net/servers/lanman* directory.

9.3. Understanding the lanman.ini File

The *lanman.ini* file is a configuration file found in the */usr/net/servers/lanman* directory on all servers. This file can be used to configure various aspects of server operations to best suit your network environment.

This section contains the following information about the *lanman.ini* file:

* The syntax of the *lanman.ini* file.
* The organization of the *lanman.ini* file.

* The sections of the *lanman.ini* file.

* A sample *lanman.ini* file.

Each of these topics is discussed in the following sections.

9.3.1. The Syntax of the lanman.ini File

The *lanman.ini* file uses the following syntax:

* The title of each section is enclosed in brackets (for example, [title]).

* The name of each parameter is at the beginning of a line, followed by an equal sign and the actual value assigned to the parameter (for example, *parameter = value*). There can be any number of spaces before and after the equal sign.

* Comments start with a semicolon (;).

* Values to parameters that are expressed as lists must be separated by commas.

* In some cases, the value of a parameter may consist of a pathname. These pathnames do not always have to be the complete UNIX system pathnames. Some parameters use *relative pathnames* (the pathname begins at an agreed upon located somewhere in the server's directory hierarchy). For example, the absolute pathname of a file might be: */usr2/lanman/john/textfile*. However, if this pathname was specified relative to the /usr2/lanman directory, the relative pathname would be: *john/textfile*.

Parameters using relative pathnames follow the convention that any relative pathname is assumed to be relative to an appropriate directory, usually a subdirectory of the LAN Manager software directory. This keeps similar system files in the same directory. See the descriptions of individual parameters to find out if relative pathnames are used, and if so, what directories they are related to.

If a parameter has no assigned value (nothing to the righ of the equal sign), the value is 0 for parameters that require a number and a null (blank) for parameters that require a character string. This may not be a legal value for the parameter. For example, the *auditing=* parameter must have either *yes* or *no* as its value; a null value prevents the server from starting.

The following is an example of the *lanman.ini* file syntax:

```
userpath=/usr/lanman  ;  default path for user home directories
```

Note: Not all parameters appear in the *lanman.ini* file. Typically, the only parameters that will appear are those that have been set to some value other than the default value. If a parameter does not appear in the file, assume that it is set to the default value.

9.3.2. The Organization of the lanman.ini File

The *lanman.ini* file consists of six sections, each containing parameters related to a part of the Server Program.

The *lanman.ini* sections are:

* *[server]*. Contains parameters common to LAN Manager servers from all vendors.
* *[lmxserver]*. Contains parameters unique to LAN Manager products derived from the AT&T LAN Manager server.
* *[workstation]*. Contains parameters used to identify the server's langroup.
* *[netlogon]*. Contains parameters for logon validation.
* *[uidrules]*. Contains parameters that specify the rules governing the mapping of server program users to UNIX system user ids.
* *[ups]*. Contains parameters that specify how the server will react in the event of a power failure.

When you start the Server Program, it reads its *lanman.ini* file for parameter values. Some of the parameters can be changed while the server is running, using the UNIX-program *svrconfig*. For others to take effect, you must stop and restart the Server Program after you have written the changes in the *lanman.ini*.

The following sections describe the parameters (and their appropriate values) found in each section of the *lanman.ini* file.



9.3.3. The *[server]* Section of the lanman.ini File

The *[server]* section contains the following parameters:

Parameter	**Function**
accessalert=	Sets the number of resource access violations that can occur before the server will send an alert message. This parameter applies to servers working in user-level security mode only. Reduce this number if tight server security must be maintained. *Minimum value*: 0 *Maximum value*: unlimited *Default value*: 5
alertnames=	Lists the usernames, separated by commas, that will receive administrative alert messages. Do not use groupnames with this parameter. *Default value*: admin *Other choices*: any valid username
auditing=	Specifies whether to start the server with the Audit Trail feature enabled or disabled. *Default value*: no *Other choice*: yes
autodisconnect=	Sets the time, in minutes, the server will wait before disconnecting an inactive session. The value 0 means that the server never disconnects an inactive session. *Minimum value*: 0 (never) *Maximum value*: 3600 minutes *Default value*: 0 (never)
erroralert=	Sets the number of errors that can occur before the server sends an alert message. Alert messages will be sent to the users specified with the *alertnames=* parameter. Reduce this number if you need rapid notification when errors occur. *Minimum value*: 0 *Maximum value*: unlimited *Default value*: 5
listenname=	Specifies the name of the server on the network. Values for this parameter may have a maximum of 8 alphanumeric

characters and must end with the *.serve* extension (for example, *adm.serve*).

If no value is given the server will be known as *uname.serve*, where *uname* is the UNIX system node name of the server computer. If you change the value of this parameter, clients attempting to access the server will have to supply the new name.

logonalert=

Sets the number of logon violations that can occur before the server will send an alert message. Alert messages will be sent to the users specified with the *alertnames=* parameter. This parameter applies to servers running user-level security only. Reduce this number if tight server security must be maintained.

Minimum value: 0
Maximum value: unlimited
Default value: 5

maxauditlog=

Sets the maximum size of the audit log file, in KBytes. When the size of the log file reaches this value, no more audit messages will be saved in the log file. Message saving will start again as soon as the log file is cleared. Reduce this number if you do not need extensive audit information.

Minimum value: 0 KBytes
Maximum value: unlimited
Default value: 100 KBytes

maxclients=

Sets the absolute maximum number of clients the server can support simultaneously. This parameter should be limited by the number of user permits purchased for this server. This parameter has an influence on the distribution of client per *lmx.srv* process and the number of *lmx.srv* processes. (See the parameter *vcdistribution* under the *[lmxserver]* section, p.9-26.)

Minimum value: 1
Maximum value: unlimited
Default value: 32

maxerrlog=

Sets the maximum size of the error log file, in KBytes. When the size of the log file reaches this value, no more error messages will be saved in the log file. Message saving will start again as soon as the log file is cleared. Reduce this number if you do not need extensive error information.

Minimum value: 0 KBytes
Maximum value: unlimited
Default value: 100 KBytes

security=

Specifies the resource security operating mode of the server. Since the server's security mode influences how the server should be set up, do not arbitrarily change this parameter's value.

Default value: user (for user-level security)
Other choice: share (for share-level security)

srvannounce=

Specifies the rate, in minutes, at which the server will announce its presence on the network. This parameter only takes effect if the *srvhidden=* parameter is set to *no*

Minimum value: 1 second
Maximum value: unlimited
Default value: 60 seconds

srvcomment=

Sets the descriptive identifier for this server, which can be seen by other computers in the server's LAN group (by using either the Full Screen Net Interface *view* menu or the Command Line Net Interface *view* option). Unlike other *lanman.ini* file parameters, the value of this parameter is not converted to uppercase letters. Up to 48 alphanumeric characters are permitted.

Default value: Supermax LAN Manager/X Server
Other choice: any valid characters

srvheuristics=

Has no effect on server operation. Provided to support the NetServerGetInfo API call only.

srvhidden=

Specifies whether or not the server will be hidden from any listing of available network servers. The default value is *no*, meaning the servername will not be hidden.

Default value: no
Other choice: yes

userpath=

Sets the pathname to the directory holding the user home directories. If a pathname used in this section does not start with a drive name or a backslash, it is assumed to be relative to the */usr/lanman* directory. On servers with a */usr2* file system, the default value is */usr2/lanman*. On all other servers, the default value is */usr/lanman*.

The directory specified by this parameter is used to hold home directories only for new users who do not already have a UNIX system login on the server. If the user does have a UNIX system login, the system will use the user's established home directory.

Your choice for this directory may be determined by where in the server's file system there is adequate space for new users. It may also be influenced by your backup procedures.

Table 9-1 lists the *lanman.ini* file's *[server]* section parameters that require numeric values. Table 9-2 lists the *lanman.ini* file's *[server]* section parameters that require character values.

Table 9-1. Parameters in the *[server]* Section that Require Numeric Values

Parameter	Minimum	Maximum	Default
accessalert=	0	unlimited	5
autodisconnect=	0 minutes	3,600 minutes	0 minutes
erroralert=	0	unlimited	5
logonalert=	0	unlimited	5
maxauditlog=	0 KBytes	unlimited	100 KBytes
maxclients=	1	unlimited but dependent on number of user permits	32
maxerrorlog=	0 KBytes	unlimited	100 KBytes
svrannounce=	0 minutes	unlimited	60 minutes

Table 9-2. Parameters in the *[server]* Section that Require Character Values

Parameter	Choices	Default
alertnames=	valid usernames (up to 128 characters)	admin
auditing	yes, no	no
listenname=	(valid name)	*uname*.serve
security=	user, share	user
svrcomment=	48 characters	Supermax LAN Manager/X Server
svrheuristics*=	(16 digits binary code)	(null)
svrhidden=	no, yes	no
userpath=	valid path	*/usr/lanman*

* Has no effect on server operation

9.3.4. The [lmxserver] Section of the *lanman.ini* File

The *[lmxserver]* section contains the following parameters:

Parameters	**Function**
accessfile=	Specifies the name of the server's *accounts* file, relative to the */usr/net/servers/lanman* directory. This file contains information about users, user groups, and access permissions for shared resources on the server. *Default value: accounts.lmx*
accessgroup=	The UNIX system group name for the server's *accounts* file. *Default value:* DOS----
accesshi=	Specifies the value the server will assign to the *accessalert=* parameter if the *alertthresh=* parameter is set to *high* . *Minimum value*: 0 *Maximum value*: 20000 *Default value*: 20000
accesslow=	Specifies the value the server will assign to the *accessalert=* parameter if the *alertthresh=* parameter is set to *low*. *Minimum value*: 0 *Maximum value*: 5 *Default value*: 5
accessmed=	Specifies the value the server will assign to the *accessalert=* parameter if the *alertthresh=* parameter is set to normal *Minimum value*: 0 *Maximum value*: 200 *Default value*: 200
accessowner=	Specifies the UNIX system owner name for the server's *accounts* file. *Default value*: *lanman*
accessperms=	Specifies the UNIX system permissions that the server's *accounts* file will receive. *Default value*: 0644

admingroupid= When the server executes an administrative command using the NetServerAdminCmd API, it must assign a group id to the executed process. This is the assigned group id. The main execisor of this API is the **net admin /c** command.

Default value: DOS----

adminpath= Specifies the path used to find commands submitted by the NetServerAdminCmd API.

Default value: */bin:/usr/bin*.

adminuserid= When the server executes an administrative command using the NetServerAdminCmd API, it must assign a user id to the executed process. This is the assigned user id. The main execisor of this API is the **net admin /c** command.

Default value: *lmxadmin*

alertthresh= Sets the frequency by which alerts are generated. Alerts are sent to the users specified with the *alertnames*= parameter.

This parameter should not be changed. Instead, change the *accessalert*=, *erroralert*= and *logonalert*= parameters. Change all three parameters at the same time, e.g. using the values *5*, *200* and *20,000* for *low*, *normal* and *high* respectively.

Default value: normal
Other choices: low, high

For the fewest alerts, set this parameter to *high*.

anncmailslot= Specifies the name of the mailslot used for periodic server announcements.

Default value: **MAILSLOT**LANMAN*

audlogfilename= Specifies the name of the Server Program's audit log file, relative to the */usr/net/servers/lanman* directory.

Default value: *logs/net.aud*.

audloggroup= Specifies the UNIX system group name (as it appears in the */etc/passwd* file) for the Server Program's audit log file.

Default value: *DOS----*

audlogowner= Specifies the UNIX system owner name (as it appears in the */etc/passwd* file) for the Server Program's audit log file.

Default value: *lanman*

audlogperms= Specifies the UNIX system permissions that the Server Program's audit log file will receive.

Default value: *0664*

byemessage= If the server is going to terminate for any reason other than a normal shutdown, it can send a popup message to all of the workstations in the langroup. If this keyword is set to *yes*, then the server will send the message.

Default value: *yes*

checkpoint= If the server has been specially compiled, it includes probes to help with performance monitoring, and must be linked aginst an appropriate library to make the probes work. This keyword tells the server whether it should make calls to the *perfhook* subroutine for performance monitoring.

Default value: *no*

clispooltime= Specifies an amount of time considered to be too long to print a job.

Default value: 20 minutes.

clstructs= This is the maximum number of different clients that can be viewed by all of the server activity monitors which are simultaneously running on the server computer.

Default value: 16

controllock= The name of the lock that is used by *lmx.ctrl* to make sure that only one *lmx.ctrl* process is running.

Default value: *.LCK.ctrl*

copyright= Is the copyright string displayed by the server.

Default value: Copyright© 1988, 1989, 1990 by AT&T and Microsoft

cpipgroup= The UNIX group for the control pipe used to contact the *lmx.ctrl* process.

Default value: *sys*

cpipname= The name of the control pipe used to contact the *lmx.ctrl* process.

Default value: *.ctrlpipe*

cpipowner= The UNIX owner for the control pipe used to contact the *lmx.ctrl* process.

Default value: *lanman*

cpipperms= The UNIX permissions that the control pipe to the *lmx.ctrl* will receive. This pipe is used by server side applications that use some of the server side APIs.

Default value: 0660

createhomedir= When a user is added to the Supermax LAN Manager/X server, the administrator can specify a home directory for that user. If the directory does not exist, and this keyword is set to *yes*, then the server creates the directory automatically.

Default value: *yes*

debug= Specifies whether debugging is on (*yes*) or off (*no*).

Default value: *no* (debugging off)
Other choices: *yes* (debugging on)

debugdir= Specifies the name of the directory, relative to the */usr/net/servers/lanman* directory, where debugging files will be stored.

Default value: none
Other choices: any valid UNIX system directory

debugpat= Debug output lines include the name of the source file that generated the debug output. This keyword allows you to set a series of regular expression filters for the output line. These regular expressions are white space separated; expressions that begin with *!* exclude the matched file names.

Default value: *

debugsignal= If this keywoprd is set to *yes*, a kill -16 will toggle the debug state of an *lmx.srv* or *lmx.ctrl* process.

Default value: *no*



debugsize=

Specifies the maximum size, in KBytes, of the debug files. When a debug file reaches this size, it is automatically truncated.

Default value: 1024 KBytes

dirbufsize=

When the server is scanning directories on behalf of a client, it allocates a buffer to hold the contents of the directory. This keyword tells the server how big a buffer to allocate (in bytes).

Default value: 4096

dirperms=

Specifies the UNIX system permissions that newly created directories will receive.

Default value: 0775

errlogfilename=

Specifies the name of the error log file, relative to the */usr/net/servers/lanman* directory.

Default value: *logs/net.err*

errloggroup=

Specifies the UNIX system group name (as it appears in the */etc/passwd* file) for the error log file.

Default value: *DOS----*

errlogowner=

Specifies the UNIX system owner name (as it appears in the */etc/passwd* file) for the error log file.

Default value: *lanman*.

errlogperms=

Specifies the UNIX system permissions for the error log file.

Default value: 0664

errorhi=

Specifies the value the server will assign to the *error-alert=* parameter if the *alertthresh=* parameter is set to *high*

errorlow=

Specifies the value the server will assign to the *error-alert=* parameter if the *alertthresh=* parameter is set to *low*.

errormed=

Specifies the value the server will assign to the *error-alert=* parameter if the *alertthresh=* parameter is set to a *normal*.

fileperms=

Specifies the UNIX system permissions that newly created files will receive.

Default value: 02664

gcbuffer= Specifies the amount of buffer space, in KBytes, allocated by each server process for client file buffering.

Default value: 100 KBytes

getapipe= Several server side programs must contact the *lmx.ctrl* process using the *getapipe* API call. This keyword indicates how long, in seconds, *getapipe* should wait for the *lmx.ctrl* server process to respond to the attempt to contact it.

Default value: 10 seconds.

hashsize= The server keeps a hash table in shared memory to keep track of the various modes that DOS and OS/2 clients have used to open files and set record locks. This keyword indicates how many buckets the hash table should have - bigger is better up to a point. It must be a power of 2.

Default value: 128.

hiprimailslot= The DOSWriteMailslot API includes a parameter to set the priority of transmitted mailslots. On the server, this means that the transmissions will be sent as high priority *STREAMS* messages (*STREAMS* is a communications facility of the UNIX operating system). Such messages, however, bypass all *STREAMS* buffering rules. This can cause problems under a heavy data flow. This parameter specifies whether the server should use high priority *STREAMS* messages.

Default value: *no*
Other choices: *yes*

ignoreunix= Setting this keyword to *yes* causes the server to completely ignore UNIX file and directory permissions.

Default value: *no*.

ipctries= There is a lot of inter-process communications between the Supermax LAN Manager/X server processes. The server uses the *read* system call to receive these IPC messages, but *read* does not always return the entire message. To ensure that the server does not keep trying forever to get an IPC message, at the expense of other activities the process could be doing, each server process checks every *ipctries read* attempt to see if other work could be done by the server.

Default value: 5

keepadmshares= If set to *yes*, this prevents remote administrators from removing the *ADMIN$* and *IPC$* shared resources.

Default value: *yes*

listenextension= This is the extension that the UNIX System V listener program, by default, applies to the *uname* of the server computer.

Default value: *.SERVE* .

lmxmsgfile= The name of the message file that the LMX server uses.

Default value: *lmx.msg*

lmxsrv= The name of the program started by *lmx.ctrl* to handle clients.

Default value: *lmx.srv*

logonhi= Specifies the value the server will assign to the *logon-alert=* parameter if the *alertthresh=* parameter is set to *high*

logonlow= Specifies the value the server will assign to the *logon-alert=* parameter if the *alertthresh=* parameter is set to *low*.

logonmed= Specifies the value the server will assign to the *logon-alert=* parameter if the *alertthresh=* parameter is set to *normal*.

lptmpdir= Specifies the full name of the directory used for placing requests to the Line Printer Spooling System (*lp*).

Default value: */usr/spool/lp/temp*

mailslotgroup= Specifies the UNIX system group name (as it appears in the */etc/passwd* file) for mailslots created on the server.

Default value: DOS----

mailslotowner= Specifies the UNIX system owner name (as it appears in the */etc/passwd* file) for mailslots created on the server.

Default value: lanman

mailslotperms= Specifies the UNIX system permissions that newly created *mailslot* file system entries will receive.

Default value: 0222

maxadminoutput=

Specifies the maximum amount of output (in KBytes) that a NetServerAdminCommand API is allowed to produce.

Minimum value: 1 KByte
Maximum value: 64 KBytes
Default value: 20 KBytes

maxfilesize=

Specifies the maximum size file (in KBytes) that a client can create on the server.

Minimum value: 100 KBytes
Maximum value: unlimited
Default value: 20000 KBytes

maxlocknap=

The longest amount of time, in seconds, that a server process will wait for a shared memory lock to become available.

Default value: 300 seconds.

maxmsdepth=

When mailslots are created, the server deletes mailslot nodes in the mailslot directory that are obsolete. It descends the directory tree below the mailslot directory up to a depth of *maxmsdepth* directories.

Default value: 5.

maxmsgsize=

This is the maximum amount of data a core client can exchange with the server.

Default value: 4356.

maxmux=

The original SMB dialect only allowed one SMB to be handled per client at a time. In other words, a particular client could not submit an SMB request until the previous one had been finished by the server. With the new dialects, the client can potentially submit several SMBs and the server will work with them as best it can. This keyword specifies the maximum number of outstanding SMBs that any one client can have at a time.

Default value: 3.

maxreadsize=

Each LAN Manager *lmx.srv* process handles more than one client at a time. If a client submits a very large read request to the server, the server will spend a lot of time fulfilling the read and other clients connected to the same *lmx.srv* process may see slow response. One solution to this problem is for *lmx.srv* to fulfill the large read in *chunks* and allow other

clients to be serviced between *chunk* reads. This keyword determines the *chunk size* in bytes.

Default value: 8192.

maxvcperproc= This is the maximum number of virtual circuits that each *lmx.srv* should be able to handle, no matter what. This is normally calculated on the fly by the server using the *vcdistribution* and *maxclients* keywords. If this keyword is non-zero, then its value is used (instead of the calculated value).

Default value: 0.

maxwritesize= The same problem described above for the *maxreadsize* keyword also exists for very large writes to the server. This keyword gives the *chunk size* for writes.

Default value: 8192.

minpassword= Specifies the minimum number of characters that may be used in a password for this server. Any password associated with a resource or a user account on this server must have at least the number of characters specified here.

Minimum value: 0
Maximum value: 14
Default value: 0

minvcperproc= This is the minimum number of virtual circuits that each *lmx.srv* should be able to handle, no matter what. This is normally calculated on the fly by the server using the *vcdistribution* and *maxclients* keywords. If this keyword is non-zero, then its value is used (instead of the calculated value).

Default value: 2

msdirgroup= Specifies the UNIX system group name (as it appears in the */etc/passwd* file) for the mailslot directory.

Default value: *DOS----*

msdirname= Specifies the name of the mailslot directory on the server, relative to the */usr/net/servers/lanman* directory.

Default value: *mailslot*.

msdirowner= Specifies the UNIX system owner name (as it appears in the */etc/passwd* file) for the *mailslot* directory.

Default value: *lanman*.

msdirperms= Specifies the UNIX system permissions for the *mailslot* directory.

Default value: 0777

msgheader= The Alerter service sends a lengthy text header when-ever it sends a message over the network. The Supermax pop-up message service cannot process long messages. This parameter specifies whether or not the header should be included with such messages.

Default value: *no* (not included)
Other choices: *yes* (included)

nethelpfile= The name of the help file that the UNIX command **net** uses.

Default value: *net/net.hlp*

netlogon= Specifies whether this server is acting as a logon validator. The *centralized*= parameter determines the type of logon validation that will be used (centralized or distributed).

Default value: *no*
Other choices: *yes*

netmsgfile= The name of the other help file that the UNIX **net** command uses.

Default value: *net/net.msg*.

netosmsgfile= The name of the message file for OS/2 error codes for the UNIX **net** command.

Default value: *net/oso001.msg*.

network= The network device names and NeTBIOS name passing type for the network(s) the server should use.

Supermax LAN Manager/X Server is able to use more networks and run over different protocol stacks simultaneously.

Each network the server should use should be specified by the special device name for the network's connection-oriented service (virtual circuit), followed by a comma and the special device name for the networks connectionless service (datagram circuit) followed by a comma and the NetBIOS name passing

type. The specification for each network to be used should be separated by a space.

The name passing types are:

0 for NetBIOS over TCP/IP
1 for TOPNetBIOS (the OSI-specification)
2 for NetBEUI

During installation of the LM/X Server, the *network=* parameter in the *lanman.ini* file will be set according to the administrator's answer when asked which type of network he wants LM/X to use.

Other choices: */dev/*<cots>, */dev/*<clts>,<type> ...

newusershell=

Specifies the login shell assigned to any new user added to the UNIX system by the Server Program. The default setting (*/bin/false*) will prevent new users from being able to login to the UNIX system (using terminal emulation). If you want new users to be able to log in to the server's UNIX system, you should specify a real shell that is available on the system (for example, */bin/sh*).

Default value: */bin/false*.
Other choices: pathnames for valid UNIX system shells

If you change this parameter, you will also have to change the new user's password.

nfslocks=

If the *unixlocks* keyword is set to *yes*, the server tries to set UNIX record locks in files as requested by clients. However, if the server is running with NFS, record locks might not work on NFS files. This keyword indicates whether or not the server should "care" if NFS record locks fail.

Default value: *no* (i.e. don't care).

nonexistusers=

When the alerter tries to send a popup message to a client on the network, NETBIOS name resolution can cause unwanted delays, if the client being accessed is not on the network. To circumvent this problem, the alerter caches the names of clients that are not up. This keyword gives the number of clients that are in this cache. Alerts will not be sent to clients that are in this cache.

Default value: 10.

nosendtime=

Related to the *nonexistusers* keyword above, this keyword gives the length of time in seconds entries will be allowed to live in the "not on the network" cache. Alerts will not be sent to clients that are in this cache.

Default value: 120 seconds.

packageid=

A one letter identifier to identify the shared memory segment needed by the server.

Default value: L

passmgmt=

Specifies the name of the program the server will use to add users to the UNIX system. If you change this parameter value from the default, the new program that is specified must emulate the passmgmt program.

Default value: */usr/bin/passmgmt*
Other choices: programs meeting the requirements above

If you do not want the Server Program to add users to the UNIX system, enter */bin/false* for this parameter.

prodname=

Is the product name of the server.

Default value: Supermax LAN Manager/X Server.

qsched=

The LMX checks every so often to see if any print queues need to be started because of the *start time* parameters associated with the queue share. This keyword indicates, in minutes, how often the server should check.

Default value: 10 minutes.

queuealloc=

The tasks in the server communicate with message queues. The items placed in these queues are allocated with the *malloc* UNIX routines. For efficiency, they are allocated in bulk - not one at a time. This keyword indicates how many should be allocated at a time.

Default value: 10.

rdatrend=

The LMX does read ahead if it detects that the client is sequentially accessing a file. It needs to observe at least *rdatrend* sequential accesses before it thinks that it should try to do readahead.

Default value: 2.



relmajor=

Specifies the major release number of the Server Program, as returned by the NetServerGetInfo API.

Default value: 1

relminor=

Specifies the minor release number of the Server Program, as returned by the NetServerGetInfo API.

Default value: 0

sbstelladmin=

When the server exceeds the maximum allowable number of clients, it can raise an administrative alert. This keyword indicates whether or not this alert should be raised. This alert results in a message being sent to the administrator.

Default value: *yes*

sbstelluser=

When the server exceeds the maximum allowable number of clients, it can send a message to the client that tried to link (but failed). This keyword indicates whether or not the message should be sent.

Default value: *yes*

sharefile=

The name of the share file for the server to use, relative to the */usr/net/servers/lanman* directory.

Default value: *sharefile*.

sharegroup=

The UNIX group name for the server's share file.

Default value: *other*.

shareowner=

The UNIX owner name for the server's share file.

Default value: *lanman*.

shareperms=

The UNIX permissions that the share file will receive.

Default value: 0644.

shmgroup=

The Supermax LAN Manager/X server needs to create a shared memory segment to allow the various server processes to share state. This is the group id of the shared memory segment.

Default value: *sys*.

shmowner=

The Supermax LAN Manager/X server needs to create a shared memory segment to allow the various server processes to share state. This is the user id of the shared memory segment.

Default value: lanman.

shmperms=

The Supermax LAN Manager/X server needs to create a shared memory segment to allow the various server processes to share state. This is the permissions assigned to the shared memory segment.

Default value: 0664.

spareserver=

The LMX ensures that an *lmx.srv* process is always available and ready to take on another client. In particular, it may start up an *lmx.srv* process that may have no clients and it is just waiting for a new one. This keyword determines if the server should always try to have a spare *lmx.srv* around.

Default value: *yes*.

spipe=

The name of the device that can be used to generate streams pipes.

Default value: */dev/spx*

srvstathelpfile=

This is the name of the help file used by the Activity Monitor.

Default value: *status/Text.mon*

srvstatmsgfile=

This is the name of the strings file used by the Activity Monitor.

Default value: *status/svrstat.msg*

stacksize=

This is the size of the stack that each task internal to the server will receive.

Default value: 10000

startscript=

Specifies the name of the UNIX system shell script run by *lmx.ctrl* when the server is started, relative to the */usr/net/servers/lanman* directory.

Default value: *lmxstart*



stoponcore=

If the *lmx.ctrl* process finds that an *lmx.srv* process unexpectedly terminated, this keyword determines if *lmx.ctrl* should stop so somebody will notice.

Default value: *yes*

svcinit=

Specifies whether or not the Server Program should run the service starter script.

Default value: *yes*
Other choices: *no*

svcscript=

Specifies the name of the script used to start Server Program services, relative to the */usr/net/servers/lanman* directory.

Default value: *lmxsvc*
Other choices: valid server starter scripts

threshold=

If the server is specially compiled, its internal tasking mechanism periodically checks to see if the internal stacks are getting close to overflowing, if it has been compiled with this particular debug feature. This keyword tells the internal checker how close a stack should get to the overflow condition before emitting warnings.

Default value: 500 bytes

uexecaccadd=

Specifies how **uexec** privileges are assigned. On user- level security servers, this parameter enables **uexec** privileges for new users. On share-level security servers, this parameter enables **uexec** privileges for new shared directories. For all servers, the parameter operates as follows:

* If set to *automatic*, **uexec** privileges are assigned automatically to each new user account (user-level security) or shared directory (share-level security).

* If set to *manual* **uexec** privileges must be assigned manually to each new user account (user-level security) or shared directory (share-level security).

Default value: *automatic*
Other choice: *manual*

unixlocks=

Specifies whether or not record locks created by DOS or OS/2 programs are reflected in the UNIX system file system. This parameter is important if there is much interaction between DOS and OS/2 versions of a program.

Default value: *yes*
Other choices: *no*

userremark= Specifies the comment that will be associated with the *users* shared resource.

Default value: *Logon Users Directory*
Other choices: any valid character string

ustructs= Specifies the number of structures allocated in shared memory to handle record lock and open file records.

Minimum value: 1
Maximum value: unlimited
Default value: 1000

uxclosecount= The server uses a technique called *file descriptor multiplexing* to allow clients to open far more files than the UNIX per-process limits would normally allow. If the server hits the per-process limit, it transparently closes the least recently accessed *uxclosecount* files to avoid hitting the per-process limit the next time a file must be opened.

Default value: 5

vcdistribution= The architecture of the server allows multiple clients to be served by each *lmx.srv* process on the UNIX system. The server must decide if a new client should be handed off to an existing *lmx.srv* process or if a new *lmx.srv* process should be started. This keyword tells the LAN Manager how to distribute clients over the *lmx.srv* processes. The value of this keyword consists of sets comma separated integers. Each set has three numbers. The first number indicates the number of clients, the second is the minimum number of VCs each *lmx.srv* should support, the third is the maximum number of VCs each *lmx.srv* should support. Her is how to interpret the default below:

Client Range	Min. clients per *lmx.srv*	Max clients per *lmx.srv*
1-16	2	4
17-25	2	5
26-36	2	6
37-49	2	7
50+	3	10

Default value: 1, 2, 4; 17, 2, 5; 26, 2, 6; 37, 2, 7; 50, 3, 10.

Table 9-3 lists the *lanman.ini* file's *[lmxserver]* section parameters that require numeric values. Table 9-4 lists the *lanman.ini* file's *[lmxserver]* section parameters that require character values.

Table 9-3. Parameters in the [lmxserver] Section That Require Numeric Values

Parameter	Minimum	Maximum	Default
accesshi=	0	20000	20000
accesslow=	0	5	5
accessmed=	0	200	200
accessperms=	0	unlimited	0644
audlogperms=	0	unlimited	0644
clstructs=			16
cpipperms=			1024
debugsize=	1	unlimited	1024
dirbufsize=			4096
dirperms=	0	unlimited	0775
errlogperms=	0	unlimited	0644
errorhi=	0	20000	20000
errorlow=	0	5	5
errormed=	0	200	200
fileperms=	0	unlimited	02664
gcbuffer=	1	unlimited	100
getapipe=			10
hashsize=			128
ipctries=			5
logonhi=	0	20000	20000
logonlow=	0	5	5
logonmed=	0	200	200
mailsotperms=	0	unlimited	0222
maxadminoutput=	1	64	20
maxfilesize=	100	unlimited	20000
maxlocknap=			300
maxmsdepth=			5
maxmsgsize=			4356
maxmux=			3
maxreadsize=			8192
maxwritesize=			8192
maxvcperproc=			0
minpassword=	0	14	0
minvcperproc=	1	30	2

Parameter	Minimum	Maximum	Default
msdirperms=	0	unlimited	0777
nonexistusers=			10
nosendtime=			120
qsched=			10
queuealloc=			10
rdatrend=			2
relmajor=	0	unlimited	1
relminor=	0	unlimited	0
shareperms=			0644
shmperms=			0644
stacksize=			10000
threshold=			500
ustructs=	1	unlimited	2500
uxclosecount=			5
vcdistribution=			1,2,4; 17,2,5; 26,2,6; 37,2,7; 50,3,10

Table 9-4. Parameters in the [lmxserver] Section That Require Character Values

Parameter	Choices	Default
accessfile=		*accounts.serve*
accessgroup=		*DOS----*
accessowner=		*lanman*
admingroupid=		*DOS----*
adminpath=		*/bin:/usr/bin*
adminuserid=		*lmxadmin*
alertthresh=	low, normal, high	normal
anncmailslot=		**mailslot**lan-man*
audlogfilename=		*logs/net.aud*
audloggroup=		*DOS----*
audlogowner=		*lanman*
byemessage=	yes, no	yes
checkpoint=	yes, no	no

Parameter	Choices	Default
controllock=		.LCK.ctrl
copyright=		Copyright (c) 1988, 1989, 1990 by AT&T and Microsoft
cpipgroup=		*sys*
cpipname=		*.ctrlpipe*
cpipowner=		*lanman*
createhomedir=	yes, no	yes
debug=	yes, no	no (off)
debugdir=		
debugpat=		*
debugsignal=	yes, no	no
errlogfilename=		*logs/net.err*
errloggroup=		*DOS----*
errlogowner=		*lanman*
getapipe=		10
hashsize=		128
hiprimailslot=	yes, no	no
ignoreunix=	yes, no	no
keepadmshares=	yes, no	yes
listenextension=		*.SERVE*
lmaddonpath=		*lmaddon*
lmsmsgfile=		*lmx.msg*
lmxsrv=		*lmx.srv*
lptmpdir=		*/usr/spool/lp/temp*
mailsotgroup=		*DOS----*
mailslotowner=		*lanman*
msdirgroup=		*DOS----*
msdirname=		*mailslot*
msdirowner=		*lanman*
msgheader=	yes, no	no
nethelpfile=		*net/net.hlp*
netlogon=	yes, no	yes, no
netmsgfile=		*net/net.msg*
netosmsgfile=		*net/oso001.msg*
network=		
newusershell=		*/bin/false*
nfslocks=		*no*
packageid=		*L*
passmgmt=		*/usr/bin/passmgmt*

Parameter	Choices	Default
prodname=		Supermax LAN Manager/X Server
sbstelluser=	yes, no	yes
sharefile=		*sharefile*
sharegroup=		*other*
shareowner=		*lanman*
shmgroup=		*sys*
shmowner=		*lanman*
spareserver=	yes, no	yes
spipe=		*/dev/spx*
srvstathelpfile=		*status/Text.mon*
svrstatmsghelpfile=		*status/svrstat.msg*
startscript=		*lmxstart*
stoponcore=	yes, no	yes
svcinit=	yes, no	yes
svcscript=		*lmxsvc*
uexecaccadd=	automatic, manual	automatic
unixlocks=	yes, no	yes
userremark=		*Logon Users Directory*



9.3.5. The [workstation] Section of the *lanman.ini* File

The [workstation] section contains the following parameters:

Parameter	**Function**
langroup=	Specifies the LAN group name for this server. Typically specified when installing the Server Program. *Default value*: *langroup*

9.3.6. The [netlogon] Section of the *lanman.ini* File

The [netlogon] section contains one parameter:

Parameter	**Function**
centralized=	Specifies the type of logon validation that will be used on the network. Typically specified when installing the Server Program. * Set to *no* for distributed logon validation (multiple servers validate logons). * Set to *yes* for centralized logon validation (a single server validates logons). If the netlogon= parameter is set to *no* on all of the network's servers, this parameter has no effect (logon validation does not occur). *Default value*: *no* (distributed) *Other choice*: *yes* (centralized)

9.3.7. The [uidrules] Section of the *lanman.ini* File

The *[uidrules]* section of the *lanman.ini* file specifies the rules that govern the mapping of Server Program users to UNIX system user ids. The *[uidrules]* section contains the following parameters:

Parameter	**Function**
exclude=	Prevents certain UNIX system user ids from being used as new users are added to the server. The syntax is a list of ranges or numbers separated by a comma. Other permissible values include any valid values or range of values for UNIX system user ids.

If the server is running user-level security, it will not assign server users any of the UNIX user ids specified by this parameter.

If the server is running share-level security and a disk resource is created whose "tree-top owner" has a user id within the specified values or range of values, then for operations on that resource, the effective user id of a server user shall be the user id of the UNIX account *lmxguest*.

Default value: 0 - 100

forceunique= If the server is running user-level security and this parameter is set to *yes* the Server Program will automatically create new, unique UNIX system login names and userids for new server users as they are created.

If the server is running share-level security and this parameter is set to *yes* then whenever server users perform operations on any disk resource, their default UNIX system user id will be the user id of the *lmxguest* account on the UNIX system.

Default value: *yes*
Other choices: *no*

9.3.8. The [ups] Section of the *lanman.ini* File

The [ups] section contains the following parameters:

poweraddr= Specifies the users that will receive the message specified by the *powermessage*= parameter in the event of a server power failure.

Default value: * (all users)

powermessage= Specifies a message that will be sent to the locations specified by the *poweraddr*= parameter if power to the server is interrupted. This message will be sent at intervals specified by the *powertime*= parameter.

Default value: The server has suffered a power failure. Please contact your administrator for further information.

powertime= Specifies the intervals (in minutes) that will elapse between broadcasts of the power failure message specified by the *powermessage*= parameter. If the *powertime*= parameter is set to *0*, the system will send the powerfail message only once. Any

other setting will generate the power failure message continuously at the interval specified.

Minimum value: 0 (once only)
Maximum value: unlimited
Default value: 1 minute

9.3.9. A Sample *lanman.ini* File

The following is a sample *lanman.ini* file from a server:

```
[workstation]
langroup=LANGROUP
; LAN group name
logonserver=\\mis
; computername of centralized logon server

[server]
maxclients=64
; the absolute number of clients the server can support simultaneously
userpath=/usr/lanman
; default path for user home directories
alertnames=marys,benp
; Admin alert usernames
auditing=no
; Keep audit trail yes/no
autodisconnect=120
; Autodisconnect timeout (minutes)
srvhidden=no
; Server hidden status
maxauditlog=100
; Max. size of audit trail file (Kb)
maxerrlog=100
; Max. size of error log file (Kb)
security=user
; Security mode (default is user)
srvcomment="Supermax LAN Manager/X Server"
; Server comment
accessalert=5
; Access violation alert threshold
erroralert=5
; Error alerting threshold
guestacct=GUEST
; Name of guest account

[netlogon]
centralized=yes
; Type of logon security

[lmxserver]
uexecprivs=automatic
; Assign uexec privileges automatically
maxmesslog=100
; Max. size of message log file (Kb)
netlogon=yes
; enable/disable logon validation
network=/dev/nbt,/dev/nbt,0 /dev/cots_5,/dev/clts_5,1
; the network device names and NeTBIOS name passing type for the networks
  the server should use
[uidrules]
forceunique=yes
; Automatically create new UIDs for new users
```

9.4. Changing Parameter Values in the lanman.ini File

There are two ways to change the values of parameters in the *lanman.ini* file. The first method involves using a text editor (such as *vi*) to change the value of any parameter in the *lanman.ini* file. With this method, you directly edit the parameters in the */usr/net/servers/lanman/lanman.ini* file.

The second method involves the UNIX program *srvconfig* to change the values of the parameters and make the changes have immediate effect on a running server.

This section describes how to change the values of the parameters associated with the Server Program, using either a text editor or the *srvconfig* program.

9.4.1. Changing Parameter Values with a Text Editor

To change the values of parameters in the *lanman.ini* file by using a text editor, follow these steps:

1. Log in as *root* at the server console.

2. Type `cd /usr/net/servers/lanman` and press RETURN.

   You are now working in the directory where the *lanman.ini* file is located.

3. Use a text editor (such as *vi*) to edit the *lanman.ini* file.

   Add or change the appropriate parameters in the *lanman.ini* file. Refer to the section of this chapter entitled *Syntax of the lanman.ini File*, for typographical and other conventions. Review the descriptions of each section of the *lanman.ini* file to determine each parameter's meaning and the acceptable values for each parameter. If you add parameters, be sure to place them under the appropriate section header in the file.

4. Save the *lanman.ini* file and exit the text editor.

5. To activate the changes, you must now stop and restart the Server Program. Type */usr/bin/lmx/lmxmgmt restart*, and press RETURN.

Note: After the Server Program is restarted, clients may automatically re-establish links to the server that existed before the Server Program was stopped.

9.4.2. Changing Parameter Values using the UNIX program *srvconfig*

You can use the *srvconfig* program to change some of the parameters from the *lanman.ini* file in a running LAN Manager server.

Use the following method:

1. Log in as *root* at the server console.

2. Type `cd /usr/net/servers/lanman/admin/srvconfig` and press RETURN.

   Refer to the section of this chapter entitled *Syntax of the lanman.ini File.*

3. Review the description of each section of the *lanman.ini* file to determine the meaning of each parameter and the acceptable values for each parameter. If you want to change a parameter, you can find the value of its current setting by typing:

   srvconfig -g `"section,keyword"`

   and press RETURN,

   where *keyword* is replaced by the parameter you want to change, and *section* is replaced by the name of the section which contains the parameter.

4. To change the value of a parameter, type:

   svrconfig -s `"section,keyword=value"`

   and press RETURN,

   where *keyword* is replaced by the parameter you want to change, and *section* by the name which contains the parameter.

5. If you want to change more parameters, type

   srvconfig -s "section,keyword=value""section,keyword=value"

   and press RETURN.

   srvconfig can be used with a blank separated list of "*section,keyword=value*".

6. Make sure that the parameter you have changed has got the right value by typing:

   srvconfig -g `"section,keyword"`

   and press RETURN.

Note: Not all parameter values will actually be changed, although it may appear so. For example, changing the *security* parameter in the *server* section should be avoided.

10. Commmand Directory

10.1. Overview

There are two interfaces available for administering Supermax LAN Manager/X Servers:

1. The Full Screen Net Admin Interface - a full screen, character-based administration program (available on Enhanced DOS and OS/2 clients only).

3. The Command Line Net Interface - a DOS-like command oriented language.

This chapter describes how to use the Command Line Net Interface. For instructions on how to administer a Supermax LAN Manager/X Server using the Full Screen Net Admin, see the relevant chapters of *Supermax LAN Manager/X - System Administrator's Guide*.

Typing **net** commands at the command line is especially useful if you

* are an advanced Supermax LAN Manager/X user and want a shortcut to the Full Screen Net Admin Interface.

* want to add **net** commands to batch files.

This chapter provides an alphabetical listing of all **net** commands that you can use to administer a server, with a brief description of the function of each command.

There is a reference page for each **net** command that is available exclusively to the administrator, explaining how to use the command and listing the purpose, syntax, and parameters of the command along with examples of its use.

Note: For information about commands that are available to users, see *Supermax LAN Manager/X - User's Guide*.

10.2. Using net commands

This section provides a few rules and guidelines to help you best use the **net** commands described in this chapter. For example, it tells you how to administer a Supermax LAN Manager/X server from three different locations.

This section also describes abbreviations you may use when typing **net** commands. Although the reference pages in this chapter spell out all command names, parameter names, and service names, Supermax LAN Manager/X allows you to abbreviate many of these for your convenience.



10.2.1. Administering Supermax LAN Manager/X via the Command Line Net Interface

Supermax LAN Manager/X servers can be administered via **net** commands from any of the following locations:

* the system prompt of Enhanced DOS and OS/2 clients
* the UNIX system prompt at the server console using the *net*-program
* the server console using the Command Line Administration Utility program, *lineadm*.

The following sections provide procedures for entering **net** commands from different locations.

Note: The syntax of **net** commands are the same regardless of where they are issued from.

10.2.2. From an Enhanced DOS or OS/2 Client

To perform a server administrator's task from the system prompt, use the **net admin** command in conjunction with the appropriate **net** command for the task. The following procedures describe two methods for entering the **net admin** command.

1. Log on to the network as *admin* or a user with administrative privileges bu typing:

   ```
   net logon username password
   ```

2. Enter the **net** command using one of the following methods:

   * Enter a separate **net admin** command for each **net** command you wish to execute, as follows:

     ```
     net admin servername /c command
     ```

     where *servername* is the name of the server you wish to administer and *command* is the **net** command you wish to execute.

     For example, to display statistics for a server named *acct.serve*, type:

     ```
     net admin \\acct.serve /c net statistics server
     ```

     Use this method for batch files, entering one or two administrative commands, or interspersing these commands with other commands at the system prompt.

   * Enter a single **net admin** command followed by multiple **net** commands, as follows:

```
net admin servername /c
```

where *servername* is the name of the server you wish to administer.

This version of the **net admin** command creates an administrative command shell at your client from which you may subsequently issue **net** commands. The prompt at your client changes to include the name of the server you are administering, for example, *[acct.serve]*.

Any **net** commands you type at this prompt will execute on the server you specify. For example, at the prompt, type:

```
[acct.serve] net access

[acct.serve] net print
```

where *acct.serve* is the prompt, and **net access** and **net print** are the commands.

This method is appropriate when you need to enter multiple administrative commands for the same server.

3. To exit the command shell and return to the system prompt, type:

```
exit
```

Note: To indicate the **net admin** requirement for administrative **net** commands, each command described in this chapter is preceded by the option [remote] (or [rmt]) in its syntax section.

10.2.3. From the Server Console UNIX System Prompt using the *net* program

To administer a server via the **net** commands, follow these steps:

1. Log on to the UNIX system as *lmxadmin* or *root*.

   At the *Console Login* prompt, type **lmxadmin** or **root**.

   At the *Password* prompt, type the appropriate password.

2. At the UNIX system prompt, log on to the network as *admin* or a user with administrative privileges by typing:

```
net logon username password
```

3. Enter any **net** command. For example, to display a list of this server's shared resources and their assigned permissions at the UNIX system prompt, type:

```
net access
```

10.2.4. From the Command Line Administration Utility program at the server console

You can administer any server on the network from this utility. You are not limited to administering the server to which the console is attached.

To run the command line administration utility, follow these steps:

1. Log on to the UNIX system as *admin* or *root*.

2. Type **/usr/bin/lmx/lineadm** to start the Command Line Administration Utility program.

3. At the *Servername:* prompt, enter the name of the server you want to administer and press RETURN. If you want to administer this server, you just need to accept the default servername by pressing RETURN.

4. At the *Username:* prompt, do one of the following:

   * Press RETURN to accept the default username (*admin*).

   * Enter a valid username that has administrative privileges for servers running user-level security.

5. At the *Password:* prompt, enter the appropriate password and press RETURN.

   * To administer a server running user-level security, enter the password for the username you entered in Step 4.

   * To administer a server running share-level security, enter the password for the *ADMIN$* directory.

   Note: If the *ADMIN$* directory does not have a password, any valid username will be able to administer the server.

   The appropriate command shell prompt is displayed depending on the server specified in Step 3.

6. Enter the appropriate **net** command.

7. To stop using the command line administration utility and return to the Supermax LAN Manager/X Server menu, do one of the following:

   * If the server you specified in Step 3 is a Supermax LAN Manager/X server, type **exit** and press RETURN.

   * If the server you specified in Step 3 is running version 3.2a or earlier of the Server Program, type **q** and press RETURN.

The *Supermax LAN Manager/X Server* menu appears.

10.2.5. Abbreviations

The following sections give examples of abbreviations for service and parameter names.

10.2.5.1. Service names

Supermax LAN Manager/X allows you to use abbreviations and synonyms for the following LAN Manager services:

Service	Acceptable abbreviations, synonyms
Workstation	wksta, work, redirector, redir, rdr,prdr, devrdr
Messenger	msg, receiver, rcv
Server	srv, svr

10.2.5.2. Parameter names

Supermax LAN Manager/X also allows you to type any unambiguous abbreviation for a **net** command parameter. This means you must type enough letters in the parameter's name to distinguish the parameter you choose from other parameters for that command. For example, if you are using a command whose possible parameters are **read** and **send**, you may type **/r** instead of **/read** and **/s** instead of **/send**. But, if the command's parameters are **read** and **redo**, Supermax LAN Manager/X will not accept **/r**, but will accept **/rea** for **/read** and **/red** for **/redo**.

The command reference pages in this chapter list command parameters in alphabetical order, making it easier for you to compare similar parameter names.

10.2.6. Using Passwords with Commands

Some commands require a password as a parameter. You can provide a password as a command parameter by typing the password on the same line as the command itself. For example, to use a shared resource called *plotter* on the *admin.serve* server (that requires a password) type:

```
net use lpt2 \\admin.serve\plotter kahuna
```

You can also ask Supermax LAN Manager/X to prompt you for your password, replacing the password with an asterisk (*) when you type the command. For example, you could type the following to use the same resource described above:

```
net use lpt2 \\admin.serve\plotter *
```

Supermax LAN Manager/X then displays:

```
Enter the password for \\ADMIN.SERVE\PLOTTER:
```

When you type a password at this prompt, the password does not appear as you type. This allows you to keep your password confidential, providing added security. You can use the asterisk (*) parameter with the following commands:

You can use the asterisk (*) with the following commands:

* **net admin**

* **net logon**

* **net password**

* **net share**

* **net use**

* **net user**

Depending on the command you type, Supermax LAN Manager/X may also prompt you for other pertinent information, such as your username.

Note: If you forget to type a password with a command that requires one, Supermax LAN Manager/X will prompt you for a password.

10.2.7. Using Command Confirmation

Many **net** commands require confirmation. Using the **/yes** and **/no** parameters helps expedite **net** commands. When Supermax LAN Manager/X reads one of these parameters, it does not pause to display the corresponding prompt. Instead, Supermax LAN Manager/X accepts the **/yes** or **/no** parameter as your response to the prompt. You can use **net** commands with **/yes** and **/no** parameters to create batch files that are not interrupted by Supermax LAN Manager/X prompts.

For example, if you use the **net logoff** command to log off the local area network with connections to remote shared resources intact, Supermax LAN Manager/X displays a prompt like this one:

```
You have the following remote connections:
    LPT1
Continuing will cancel the connections.
Do you want to continue this operation? (Y/N) [Y]:
```

You can use the **/yes** and **/no** parameters with any **net** command to anticipate and respond to a prompt. For example, if you include the **net logoff** command in a batch file, and know that you want to respond with a **Y** to the prompt, you can type the following line in your batch file:

```
net logoff /yes
```

10.3. Command Reference Pages

The Command Directory provides individual "reference pages" for each of the **net** commands available for administering the server. Each command reference page includes the following information:

* Command Name

  The top of each reference page shows the name of the **net** command.

* Syntax

  The command's syntax shows how to use the command: which parameters are required, which are optional, and which only work with other parameters. The conventions used to describe a command's syntax are explained in the following section, *Understanding Command Syntax*.

* Purpose

  This section provides a brief description of the command and what it does.

* Parameters

  This section explains the parameters that may be used with each command and how they affect that command.

* Comments

  This section describes how to use the command, when to use it, and why. It describes the command's parameters, and explains which parameters may be used in combination. It may also contain warnings or suggestions about using the command.

* Examples

  This section gives examples that show how the command is used.

* See Also

  This section lists the titles of command reference pages that you can read for more information about the command. Unless noted otherwise, these reference pages are contained in this chapter.

10.3.1. Understanding Command Syntax

The commands described in this Command Directory will be easier to understand and use if you keep in mind the following:

* When a command element is presented like this:



```
net access
```

you type it letter for letter.

* When a command element is presented like this:

```
servername
```

you replace it with a specific name, as appropriate for your network.

* When parameters are stacked within braces, like this:

```
{ parameter1 }
{ parameter2 }
{ parameter3 }
```

you must include one of the parameters in the command string. (Do not type the braces.)

* When a parameter is within square brackets, like this:

```
[parameter]
```

the parameter is optional. When more than one parameter is within square brackets, you may use any or all of the parameters and enter them in any order. (Do not type the brackets.)

* Brackets and braces are sometimes used together. The following example shows braces within brackets:

```
[rmt] net error [ { /count:# [/reverse] } ]
                [ { /delete           } ]
                [ { /reverse          } ]
```

This combination of braces and brackets indicates that, although the parameters are optional, if you do use a parameter, you must select only one of them. You could use either of the following variations:

```
net error
net error /count:# /reverse
net error /count:#
net error /delete
net error /reverse
```

* Be sure to type slashes (/), backslashes (\), equal signs (=), colons (:), semicolons (;), and asterisks (*) as they are shown in this Command Directory. If the following characters ((semicolon (;), backslash (\), asterisk (*), and single quote (')) are entered at the UNIX system console or the interactive shell, precede them with a backslash (\).

* Replace pound signs (#) with a number.

* You can type network commands on your keyboard in upper- or lowercase letters.

* When you finish typing a command, press RETURN. If you are typing a long command string, do not press RETURN when your cursor gets to the edge of your screen; the cursor will "wrap around" and continue on the next line of your screen. Press RETURN only after you finish typing the entire command string.

Note: *rmt* used in a syntax is short for *remote*.

10.4. Commands in This Directory

The following table describes each of the **net** commands documented in this guide. Unless otherwise noted, these commands are available only to users with administrative privileges. For information on **net** commands available to all users, see *Supermax LAN Manager/X - User's Guide*.

Table 10-1. net Commands (For Administrators Only)

Command	Function
net access	Lists, creates, changes, and revokes permissions for users of resources at the server. This command works only on servers running with user-level security.
net admin	Starts the Full Screen Net Admin Interface, or allows an administrator to run a command remotely on another server.
net audit	Displays or clears the Audit Trail entries for a server.
net config server	Displays information about or changes the configuration of a server.
net continue print	Continues Supermax LAN Manager/X printers suspended by the **net pause print** command.
net device	Lists devicenames and controls shared printers.
net error*	Lists the most recent local area network errors and the times they occurred.
net file	Displays the names of all open shared files and the number of locks, if any, on each file. It also closes shared files and removes file locks.

net group	Displays the names of groups and their members and updates the group list at a server.
net load*	Loads a specified file as the new sharelist on the server.
net pause print	Suspends a printer shared by the server.
net print*	Displays and controls the contents of a shared printer queue.
net save*	Saves a copy of the current sharelist in a file on the server.
net send*	Sends messages and files to other users.
net separator	Causes a custom separator page to print between each print job for a specified printer queue or printer.
net session	Lists or disconnects sessions between the server and other computers on the local area network.
net share	Makes a resource available to clients.
net statistics*	Displays and clears a server's list of usage statistics.
net status	Displays a server's computername, configuration settings, and a list of shared resources on the server.
net user	Lists, adds, removes, and modifies user accounts on the server.

* This command provides different capabilities for users *without* administrative privileges. For information on these capabilities, see *Supermax LAN Manager/X - User's Guide*.

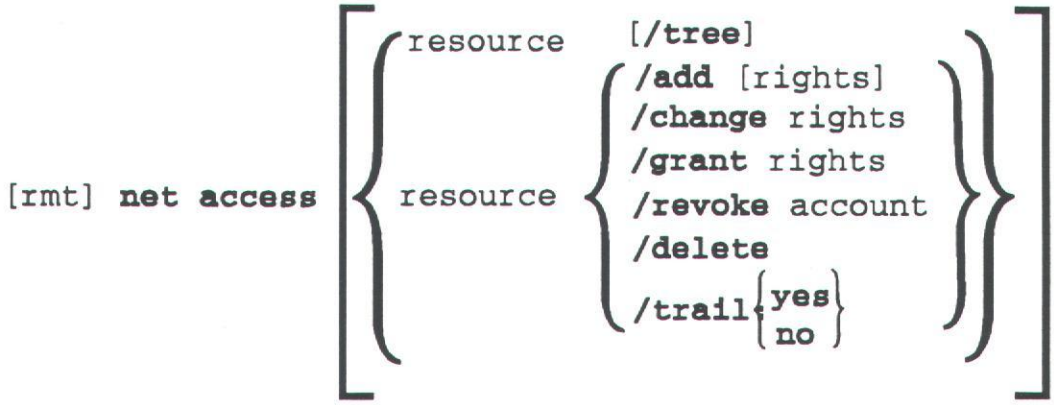
10.5. Administrative net Commands

The following section includes a reference page for each of the **net** commands that can be used to administer a server.

For **net** commands that are primarily invoked by users, see *Supermax LAN Manager/X - User's Guide*.

10.5.1. net access

Syntax



Purpose

This command lists, creates, changes, and revokes permissions for users of resources at the server. It works only on servers running with user-level security.

Before you can assign user or group permissions to access shared resources, you must first share the resources using the **net share** command. The Example section explains this process.

Parameters

remote is required only when you are entering the command from the Enhanced DOS or OS/2 client system prompt. The *remote* parameter is replaced with:

```
net admin  \\servername  /c
```

where *servername* is the name of the server you are administering.

For information on using this parameter, see the *Administering Supermax LAN Manager/X via the Command Line Net Interface* section earlier in this chapter.

resource names the full path to the resource to be assigned permissions. The resource can be a disk, directory, file, printer queue, **\print** or **\pipe**. The latter two define default access for all printer queues.

rights in the form **account:***permissions*, includes the name of a user or group account followed by the permissions (**r**,**w**,**c**,**x**,**d**,**a**,**p**,**y**,**n**) for the resource.

account identifies the username or groupname of a specific account whose permissions are being modified.

add adds user permissions for a previously unshared resource to the access-control database. If users have already been assigned permissions for the resource, and you want to add permissions for an additional user, use the **grant** parameter instead.

/change changes a user's or group's permissions for a resource.

/delete removes all permissions for a resource from the access-control database. Once permissions are deleted for a directory or file, users will not be able to access the directory or file as a shared resource.

/grant adds a new username and corresponding permissions to a pre-existing resource record.

revoke revokes a particular user's or group's permissions to use the resource. Other users with appropriate permissions may continue to access the resource.

/trail:[yes|no] turns audit trailing on or off for a particular resource. (The default is yes.)

/tree reports permissions for the resource specified and all of its descendants (for example, subdirectories of a specified directory).

When used without parameters, the **net access** command displays a list of the server's shared resources plus their assigned permissions:

```
Resource        Permissions     Permissions
-------------------------------------------------

\PRINT          BENP:W          GUEST:WC
                JOHNT:W                     MARYJ:WC
                MIKEG:WC        *USERS:WC
C:\
                GUEST:R                     *USERS:R
C:\LANMAN\SPOOL
                GUEST:R                     *USERS:R

The command completed successfully.
```

This display shows the pathname of every resource and the permissions assigned for that resource. (Groupnames are preceded by *.)

Note: If you type the **net access** command for a remote resource, the path in the Resource column is relative to the remote server, not your client.



Comments

Before you can use the **net access** command, you must:

* make sure the server is operating with user-level security
* make sure the resource exists
* have existing accounts for the users or groups for which you are assigning permissions.

When you use the **net access** command to display access permissions, a comment next to each resource's name shows whether access of that resource is being audited. Under each resource name are the names of users and groups permitted to use the resource and the specific permissions. Three types of resources can appear in the list:

1. Pathnames of drives, directories, or files
2. Sharenames of printer queues
3. Pathnames of named pipes.

The **net access** command can assign up to nine permissions. These permissions apply only when the server is running with user-level security. (For information on assigning permissions while the server is running with share-level security, see the **net share** command.) Some permissions work only with specific types of resources, as follows:

Code	Permission
r	"read" lets users read a directory's files or copy its files to other directories. It also lets users view the names of files in a shared directory. When used by itself, it allows users to look at or execute programs only.
w	"write" lets users make changes to the files in a directory. In most cases, it should be used in combination with read permission.
c	"create" lets users create files and subdirectories in a shared directory. When used by itself, it lets users create new files in the directory and change them while they are creating them. Once the file is closed, it cannot be modified.
x	"execute" lets users run a command or program.
d	"delete" allows users to delete files and subdirectories.

a	"change attributes" lets users change file attributes. For more information on file attributes, see your DOS or OS/2 documentation.
p	"change permissions" lets users change resource permissions. (This is the same as giving a user administrative privilege for a resource.)
y	"yes" allows users to submit files and requests to a printer queue.
n	"no" denies users access to a resource, and is used to exclude a specific person or persons from using a printer queue, directory, or file.

Only users who are assigned the permission "p" can change the permissions on a shared resource using the **net access** command. Otherwise, administrative privilege on your server account must be obtained before permissions for resources shared from that server can be changed.

For a resource to be audited, the **net access** command must be used with the name of the resource, and the **/trail:**-parameter must be set to **yes**. Since **yes** is the default for this parameter, if you type the **/trail:** parameter with no value, auditing is turned on.

Examples

Before you can assign user and group permissions to access shared resources, you must first share the resource using the **net share** command. From the client, type:

```
net admin \\acct.serve /c net share sharedir=c:\usr     hello
```

where *acct.serve* is the name of the server; *sharedir* is the name of the shared resource; *c:\usr* is the full path that links to *sharedir*; and *hello* is the password assigned to *sharedir*.

You can assign access permissions for users and groups to the shared resource, but first you must create the new users. Use the **net user** command as described in the following examples.

To set up a new user account for Mary Jones with user privileges, type:

```
net admin \\acct.serve /c net user maryj new /add /priv:user
```

where *acct.serve* is the name of the server; *annaj* is the username of the newly created account; *new* is the password assigned to the new user account; and *maryj* has been given user privileges.

Now you can assign access permissions for the new user on *sharedir* by typing:

```
net admin \acct.serve /c net access c:\usr /add maryj:rw
```

where *acct.serve* is the name of the server; *c:\usr* is the full path that links to *sharedir*; and the user *maryj* has been given read and write permissions on *sharedir*.

To change *maryj*'s ability to only write to subdirectories and files in *sharedir*, type:

```
net admin \\acct.serve /c net access c:\usr /change maryj:w
```

where *acct.serve* is the name of the server; *c:\usr* is the full path that links to *sharedir*; and *maryj:w* changes maryj's access permissions to write only.

See Also

For information about	See
Sharing resources with the local area network	**net share**
Adding users to the server	**net user**
Adding groups to the server	**net group**
Adding and changing permissions using the Full Screen Net Interface	*System Administrator's Guide*
Starting the server with user-level security, and assigning permissions	*System Administrator's Guide*

10.5.2. net admin

Syntax

```
net admin [\\servername [password] [{/c | /c command}]]
```

Purpose

This command starts the Full Screen Net Admin Interface or allows an administrator to run a command remotely on another server.

Parameters

servername specifies the name of the server the administrator is accessing.

password specifies the administrator's password on *servername*.

/c starts a secondary command shell or runs the command at *servername*.

command specifies the command to be run.

When you type the **net admin** command without parameters, or with *servername* only, the command starts the Full Screen Net Admin Interface.

Comments

When you start the Full Screen Net Admin Interface, you must supply the computername of the server you wish to administer. (You must have administrative privilege for the server in order to do this.) If your password for that server is different from your logon password, you must also type your password.

When you use the *command*-parameter without a following command, it starts a command processor (similar to the OS/2 *cmd.exe* command processor) that runs at the designated remote server. This command processor prompts for **net** commands, runs them, and returns the resulting output to your screen.

To exit from the command processor, type **exit**, or press CTRL+Z. You can also type the **net admin** command as follows to run a single, non-interactive **net** command at the remote server:

```
net admin  \\servername [password] /c command
```

Examples

To display a list of the server's (*acct.serve*) shared resources in addition to the assigned permissions, type:

```
net admin \\acct.serve /c net access
```

To run the Full Screen Net Admin Interface on a client, type:

net admin

See Also

For information about	See
Administering a server	*System Administrator's Guide*
Starting the Full Screen Net Interface	*Supermax LAN Manager/X - User's Guide*
Starting the Full Screen Net Admin Interface	*System Administrator's Guide*

10.5.3. net audit

Syntax

```
remote net audit [ { /count:#[/reverse] } ]
                 [ { /delete           } ]
                 [ { /reverse          } ]
```

Note: This command can only be entered from the Enhanced DOS or OS/2 client system prompt. The *remote* parameter is replaced with:

```
net admin \\servername  /c
```

where *servername* is the name of the server you are administering.

Purpose

This command displays or clears the Audit Trail entries for a server.

Parameters

/count: displays the *number* of the oldest Audit Trail entries in the log. When used with the **/reverse** parameter, it displays the *number* of the most recent entries.

/delete clears the current Audit Trail log.

/reverse displays the Audit Trail entries in reverse chronological order (newest to oldest).

When used without parameters, the **net audit** command displays the entire Audit Trail log of a server, as follows:

```
User name    Type   Date
-------------------------------------------------------------
MARYJ        Session  Oct 20, 1989 at 23:36:01
  Logoff Auto-Disconnect, Duration:  Not available
JOHNT     Session   Oct 21, 1989 at 16:27:00
  Bad Password
MIKEG        Share  Oct 22, 1989 at 17:23:47
  Use C
MaryJ                Session        Oct 22, 1989 at 17:24:47
  Logoff Normal, Duration:  0:1:0
JOHNT                Share  Oct 25, 1989 at 15:22:33
  Users' session disconnected, Duration:  0:30:19

The command completed successfully.
```

This screen displays:

Column	Contents
User name	The username of the person using the resource
Type	The type of resource in use
Date	The date and time on which use of the resource began
Duration	The length of time (*hh:mm:ss*) the resource was in use

The following are the six types of activities that can be audited:

Type	Audited activities
Server	Starting and stopping the server
Session	User sessions, logging on, logging off
Share	Adding or deleting shared resources
Access	Starting access (for example, via **net use**) of a shared resource
Access ended	Stopping access of a shared resource that is configured to be audited
Access denied	Attempts to access shared resources that failed due to bad passwords or insufficient permission

Comments

The **net audit** command reports who has used which resource on the server and how. When a server is running with user-level security, you can selectively audit individual shared resources. When a server is running with share-level security with auditing on, all shared resources are audited.

The **net audit** command reports activity for resources identified by the **/trail:yes** parameter of the **net access** command. It also reports activity for the server if you started the server with the **/auditing:yes** parameter, or if the **auditing=** parameter in the server's *lanman.ini* file is set to **yes**.

To stop auditing the server once it is started, you must restart the server with the audit feature turned off. To stop auditing a particular resource on a server running user-level security, use the **net access** command with the **/trail:no** parameter.

Supermax LAN Manager/X Audit Trail entries are logged in the server's file */usr/net/servers/lanman/logs/net.aud*. The size of your server's audit log is set by the **maxauditlog=** parameter in the server's *lanman.ini* file.

Examples
To display the entries of the Audit Trail for the server named *acct.serve* in reverse chronological order (from newest to oldest), type:

```
net admin \\acct.serve /c net audit /reverse
```

To clear all entries from the Audit Trail log for the server named *acct.serve*, type:

```
net admin \\acct.serve /c net audit /delete
```

See Also

For information about	See
Starting a server with auditing turned on	*System Administrator's Guide*
Controlling access to shared resources	**net access**

10.5.4. net config server

Syntax

```
[remote] net config server [parameters]
```

Purpose

This command displays information about or changes the configuration of a server.

Parameters

remote is required only when you are entering the command from the Enhanced DOS or OS/2 client system prompt. The *remote* parameter is replaced with:

net admin \\servername /c

where *servername* is the name of the server you are administering.

For more information on using this parameter, see the *Administering Supermax LAN Manager/X via the Command Line Net Interface* section earlier in this chapter.

The following are valid parameters for this command:

/accessalert: # specifies the number of permission violations that can occur before an alert message is sent to the users named in the **alertnames=** parameter of the *lanman.ini* file.

/alertnames:*name [;...]* specifies one or more usernames to receive alert messages (such as when there is a printer problem or when the disk is nearly full). Separate multiple usernames with semicolons (;).

/autodisconnect:*time* specifies the maximum number of minutes a user's session can be inactive before it is automatically disconnected from the server.

/erroralert:# specifies the number of errors that can occur before an alert message is sent.

/logonalert:# specifies the number of logon violations that can occur before an alert message is sent.

/maxauditlog:# specifies the maximum size, in KBytes, of the server's audit trail file.

/srvcomment: *text* specifies the comment for the server.

srvhidden:[yes | no] specifies whether the server's computername will be hidden. If the server's computername is hidden, its name does not appear on any lists of local area network servers. The default is **no**.

When used without parameters, the **net config** command displays the Supermax LAN Manager/X services that can be reconfigured on this server:

```
The following running services are configurable:

WORKSTATION  SERVER

The command completed successfully.
```

Comments

The **net config server** command allows you to make a temporary change to certain configuration settings for your server. If you intend to make a permanent change to your server's configuration, you should modify the server's *lanman.ini* file. You may also use AT&T FACE to modify some of the file's parameters.

When you type **net config server**, a display similar to the following shows configuration information about the server:

```
Server name                          \\ADMSVC
Server comment                     in Jack Starkey's office
Send admin alerts to               JOHNT

Software version                   1.0
Server active on                   NET1
Supermax Lan Manager/X root        C: LANMAN
User directories root              C: LANMAN ACCOUNTS USERDIRS

Number of net buffers               15     Server hidden          No
Size of net buffers (byte)        4096     Auditing enabled       No
Number of big buffers                2     Security mode          User

Max logged on users                 32     Alert interval (min)      5
Max concurrent admin                 2     System error limit        5
Max resource shares                 23     Net I/O error limit       5
Max resource connections           128     Passwd violation limit    5
Max open files                      64     Access violation limit    5
Max open files per session          50     Disk space limit        300
Max file locks                      64       (KByte)

Idle session time (min)            120     Max audit log size      100
                                             (KByte)

The command completed successfully.
```

This screen displays:

* the settings for the server, such as its computername, descriptive comment, default local area network, and names of users who receive alert messages.

* whether the security is user level or share level, and if auditing is on or off.

* the file and memory management used by the system, as well as the maximum number of users who can use the server and its shared resources.

* the maximum number of resources the server can share.

* the maximum number of files that can be opened at one time on the server.

* the location of the *lanman* directory and the user's home directories in the UNIX system file system on the server.

After you start the server, you can only change a configuration value associated with the **net config server** command. The following lists each **net config server** parameter and its related *lanman.ini* file entry and its related text in the display shown when you type **net config server**:

Command parameter	Equivalent lanman.ini entry	Equivalent text displayed:
/accessalert:#	accessalert=	*Access violation limit*
/alertnames:name[,...]	alertnames=	*Send admin alerts to*
/autodisconnect:time	autodisconnect=	*Idle session time*
/erroralert:#	erroralert=	*System error limit*
/logonalert:#	logonalert=	*Passwd violation limit*
/maxauditlog:#	maxauditlog=	*Max audit log size*
/srvcomment:text	srvcomment=	*Server comment*
/srvhidden:[yes|no]	svrhidden=	*Server hidden*

To permanently change these and other configuration settings for your server, change the appropriate entries in the *lanman.ini* file, then restart your server.

Examples

The audit log is growing due to the resource that is being audited. To increase the size of the audit file for *acct.serve*, type:

```
net admin \\acct.serve /c net config server /maxauditlog:#
```

where # is the maximum size of the server's audit trail file.

Too many links on the server are inactive and other users are locked out. To decrease the idle session time on *acct.serve*, type:

```
net admin \\acct.serve /c net config server /autodisconnect:
time
```

where *time* is the new (decreased) time that a user's session can remain inactive before being disconnected.

See Also

For information about	See
net config workstation	*Supermax LAN Manager/X - User's Guide*
Using the server's *lanman.ini* file	*System Administrator's Guide*

10.5.5. net continue print

Syntax

```
remote net continue print [=printername]
```

Note: This command can *only* be entered from the Enhanced DOS or OS/2 client system prompt.

The *remote* parameter is replaced with:

```
net admin \\servername  /c
```

where *servername* is the name of the server you are administering.

Purpose

This command continues Supermax LAN Manager printers suspended by the **net pause print** command.

Parameters

printername specifies the UNIX lp subsystem name for that printer. Omitting *printername* continues all print devices on that server.

Comments

The **net continue print** command can be abbreviated **net cont**.

This command reinstates printers that were paused using the **net pause print** command.

When you continue a shared printer, you allow users to once again use the printer.

Examples

To pause the printer named *hplaser*, type:

```
net admin \\acct.serve  /c net pause print=hplaser
```

where *acct.serve* is the name of the server; and *hplaser* is the name of the printer whose services are being paused.

To continue the *hplaser* printer services, type:

```
net admin \\acct.serve  /c net continue
print=hplaser
```

where *acct.serve* is the name of the server; and *hplaser* is the shared printer whose printing services are now being continued.

See Also	For information about	See
	Pausing LAN Manager services	**net pause**
	Sharing resources on the local area network	**net share**
	net continue command user's version)	*Supermax LAN Manager/X - User's Guide*

10.5.6. net device

Syntax

```
[rmt] net device [ printername [{ /restart }] ]
                                [{ /delete  }]
```

Purpose

This command lists devicenames and controls shared printers.

Parameters

remote is required only when you are entering the command from the Enhanced DOS or OS/2 client system prompt. The *remote* parameter is replaced with:

```
net admin \\servername  /c
```

where *servername* is the name of the server you are administering.

For more information on using this parameter, see the *Administering Supermax LAN Manager/X via the Command Line Net Interface* section earlier in this chapter.

printername specifies the UNIX lp subsystem printername of the device (for example, *laser* or *dde1080*).

/delete deletes the current print request.

/restart begins reprinting the current document at a spooled printer from the beginning.

When used without parameters, the **net device** command displays the status of all shared printers at the specified server.

```
Device                  Status          Time            User Name
-------------------------------------------------------------------
LPT1    Spooled         Printing        00:00:00
COM2                    Idle            00:00:00

The command completed successfully.
```

This screen displays:

Column	Contents
Device	The printername of the shared resource
Status	The status of the printer
Time	This field is not applicable and always displays zero.
User Name	The system does not display the user name.

Comments

When used with just the printername parameter, the **net device** command displays the status of the specified printer only.

Note: The name of a spooled print device is followed by the word "Spooled." Because Supermax LAN Manager/X retains information about spooled printer queues you define, you can display information about a device associated with a spooled printer queue even if that printer queue is not currently shared.

The status of a device can be one of the following:

Status	Meaning
Idle	Not currently being used
Printing	The printer is active
Paused	The device has been paused with the **net pause** command.
Error	There is a problem with the device.

Examples

To list the status of the printer (on the *acct.serve* server) with the UNIX lp subsystem printername *laser*, type:

```
net admin \\acct.serve /c net device laser
```

To delete the current print request from *laser*, type:

```
net admin \\acct.serve /c net device laser /delete
```

See Also

For information about	See
Printer queues and devices	**net print**
Sharing printer queues	**net share**

10.5.7. net error

Syntax

```
[rmt] net error [ { /count:#[/reverse] } ]
                { /delete              }
                { /reverse             }
```

Note: This command can only be entered from the Enhanced DOS or OS/2 client system prompt.

The *rmt* (remote) parameter is replaced with:

```
net admin  \\servername  /c
```

where *servername* is the name of the server you are administering.

Purpose

This command lists the most recent local area network errors and the times that they occurred.

Parameters

/count:# displays the *number* of oldest entries in the error log. When used with the **/reverse** parameter, this displays the *number* of most recent errors in the error log.

/delete removes all entries from the error log.

/reverse displays the error log entries in order of oldest to newest.

When used without parameters, the **net error** command displays the full error log of the server in chronological order. The **net error** command produces the following display:

```
Program      Message        Time
NETPOPUP     2851           Mar 07, 1989, 16:03:30
 NET2851:    Unable to display message POPUP due to
 OS/2 VIO call error
 E3 01 01 00                                    ....
WORKSTATION  2890           Mar 08, 1989, 14:13:57
 NET2890:    A NetWksta internal error has occurred:
 DecrNCBNeed: nbi_NCBneed going negative?
 3A 26                                         :&

The command completed successfully.
```

This screen displays:

Column	Contents
Program	The name of the program that encountered the error
Message	The message generated by the error
Time	The date and time the error occurred

Some error log entries may also include a raw data listing to help a technician resolve the problem.

Comments

This command also can be typed **net errors**. The text of the error log is kept in the */usr/net/servers/lanman/logs/net.err* file.

When the error list becomes full, the oldest error is deleted to make room for the next error to be added to the list.

The size of your server's error log is set by the **maxerrlog=** parameter in the server's *lanman.ini* file.

Examples

To see the error log for *acct.serve*, type:

```
net admin \\acct.serve /c net error
```

If there is no need to keep the current list, you may clear all the entries from the log by typing:

```
net admin \\acct.serve /c net error /delete
```

If you have had trouble using the server, you may need to view your error log. If your error log is quite large, you may want to view only a part of it. To display its 15 most recent entries, type:

```
net admin \\acct.serve net error /count:15
/reverse
```

Because these are the most recent entries in your log, they should be useful in troubleshooting your server.

See Also	For information about	See
	Setting the size of the error log file	*System Administrator's Guide*
	Displaying an OS/2 client's error log	*Supermax LAN Manager/X - User's Guide.*

10.5.8. net file

Syntax

```
[remote] net file [id[/close]]
```

Purpose

This command displays the names of all open shared files and the number of locks, if any, on each file. It also closes shared files and removes file locks.

Parameters

remote is required only when you are entering the command from the Enhanced DOS or OS/2 client system prompt. The *remote* parameter is replaced with

```
net admin  \\servername  /c
```

where *servername* is the name of the server you are administering. For information on using this parameter, see the *Administering Supermax LAN Manager/X via the Command Line Net Interface* section earlier in this chapter.

id specifies the identification number of a file.

/close closes an opened file and releases locked records.

When used without parameters, the **net file** command lists all the open files at a server, as follows:

```
File        Path                          User name       # locks
1           \usr\sharedir\testfile        maryj           0

The command completed successfully.
```

This screen displays:

Column	Contents
File	The identification number assigned to the open file
Path	The pathname of the open file
User name	The username of the person using the file
#locks	The number of locks on the file

You will receive one entry for each instance of an open file, therefore if a file is opened three times, you will receive three separate entries.

Comments

The **net file** command also can be typed **net files**.

The administrator has the ability to close files, which removes any locks, by using the **net file** command.

There are a number of reasons why you may need to close an opened file on the server. Sometimes you simply need to clean up after a program that left a file open. Other times, you may need to close a file with which somebody is working. For example, if you discover a security breach such as someone reading a confidential file, you can use the **net file** command with the **/close** parameter to close the file.

The locked portions of a file cannot be used by other computers on the local area network. Files sometimes are left opened and locked, usually because of a program error. When this happens, no users can access the locked portions of the file until someone removes the lock and closes the file. The **net file** command can do this.

Examples

To display additional information on an open file on the *acct.serve* server, type:

```
net admin \\acct.serve /c net file 1
```

where *1* is the file id number.

To close an open file, type:

```
net admin \\acct.serve /c net file 1 /close
```

where *1* is the id number of the file to be closed.

This command closes the file and releases any file locks, making the file available for local area network use.

See Also

For information about	See
Sharing files	**net share**
Managing files and removing file locks	Chapter 2 of this guide

10.5.9. net group

Syntax

```
[remote] net group [groupname [username1...]{ /add | /delete }]
```

Purpose

This command displays the names of groups and their members and updates the group list at a server. This command is available only on servers running with user-level security.

Before users can be added to groups, user accounts must be created on the server using the **net user** command. See the Examples section for more information.

Parameters

remote is required only when you are entering the command from the Enhanced DOS or OS/2 client system prompt. The *remote* parameter is replaced with:

```
net admin \\servername  /c
```

where *servername* is the name of the server you are administering.

For more information on using this parameter, see the *Administering Supermax LAN Manager/X via the Command Line Net Interface* section earlier in this chapter.

groupname specifies the name of the group to be added, expanded, or deleted.

username specifies one or more usernames to be added or deleted.

/add adds a group or adds members to a group.

/delete deletes a group or deletes members from a group.

When used without parameters, the **net group** command names the server and its associated groupnames, as follows:

```
User Groups for \\acct.serve
*UEXEC  *USERS
```

Comments

This command also can be typed **net groups**. It works only at servers running with user-level security.

When used with the groupname, the **net group** command displays the name of the group and its members, as follows:

```
Group Members of PUBREL
ANNM            JOHNH           KARENL
BENNYPO         MaryJ           NISH
MADST           PIASV
```

The list of groups and their members is kept in the */usr/net/servers/lanman/accounts.lmx* file.

Before creating groups or adding a user to groups, create user accounts.

Examples

To set up a new user account for Karen Andersen that gives her administrative privileges, type:

```
net admin \\acct.serve /c net user karena new /add
/priv:admin
```

where *acct.serve* is the name of the server; *karena* is the username of the newly created account; and *new* is the password assigned to this new user account.

To add a new group called *sales* to the server, type:

```
net admin \\acct.serve /c net group sales /add
```

where *acct.serve* is the name of the server; and *sales* is the name of the group.

To add usernames *karena* and *fredt* to the group, type:

```
net admin \\acct.serve /c net group sales karena fredt
/add
```

where *acct.serve* is the name of the server; *sales* is the name of the group; *karena* and *fredt* are the usernames to be added to the *sales* group. The server must already have user accounts for *karena* and *fredt*.

To display the names of members of the new group, type:

```
net admin \\acct.serve /c net group sales
```

The following display appears:

```
Group Members of SALES
KARENA          FREDT
```

To delete *fredt* from the *sales* group, type:

net admin \\acct.serve net group sales fredt /delete

where *acct.serve* is the name of the server, *sales* is the name of the group, and *fredt* is the user deleted from the group.

See Also

For information about	See
Granting groups access to shared resources	**net access**
Adding user accounts to the server	**net user**

10.5.10. net load

Syntax

```
[remote] net load filename
```

Purpose

This command loads a specified file as the new sharelist on the server. Before loading a new sharelist, the sharelist must have been saved using the **net save** command.

Parameters

remote is required only when you are entering the command from the Enhanced DOS or OS/2 client system prompt. The *remote* parameter is replaced with:

```
net admin  \\servername  /c
```

where *servername* is the name of the server you are administering.

For information on using this parameter, see *Administering Supermax LAN Manager/X via the Command Line Net Interface* section earlier in this chapter.

filename specifies the name of the file to replace the current sharelist. The file must have been created previously with the **net save** command.

Comments

The administrator can use the **net load** command to load a specified file as the new sharelist on the server. The sharelist is a binary file that contains a list of all available shared resources on a server. The file you specify with the **net load** command will replace the current sharelist. If you wish to save the current sharelist for later use, use the **net save** command first, then use the **net load** command.

Supermax LAN Manager/X loads the saved file you specified from the */usr/net/servers/lanman/profiles* directory on the server.

Users can also use the **net load** command to load profile (*.pro*) files on a client. Profile files contain lists of **net use** commands that define a client's network connections.

For more information about the user's version of the **net load** command, see *Supermax LAN Manager/X - User's Guide.*

Examples

Your department has two work shifts, each one needs access to a different set of resources on the same server. Consequently, you have created two sharelists

on the server. You must load the file called *daylist* that you created for the day shift as the current sharelist. First, save the daylist from a previously created sharelist using the **net save** command.

To save a copy of the current sharelist, type:

```
net admin \\acct.serve /c net save daylist
```

where *acct.serve* is the name of the server; and *daylist* is the name of the file containing the contents of the new sharelist file.

To load *daylist*, type:

```
net admin \\acct.serve /c net load daylist
```

where *acct.serve* is the name of the server; and *daylist* is the name of the file that contains the new sharelist file.

See Also

For information about	See
Creating sharelist files	**net save**
Using **net load** for profile files on a client	*Supermax LAN Manager/X - User's Guide*.

10.5.11. net pause print

Syntax

```
remote net pause print [=printername]
```

Note: This command can *only* be entered from the Enhanced DOS or OS/2 system prompt.

The *remote* parameter is replaced with:

```
net admin  \\servername  /c
```

where *servername* is the name of the server you are administering.

Purpose

This command suspends a printer shared by the server.

Parameters

printername specifies the UNIX lp subsystem name for the printer. Omitting *printername* pauses all print devices on that server.

Comments

Pausing provides administrators with a way of suspending Supermax LAN Manager/X printing services.

Pausing a printer makes that device unavailable to local area network users.

If a job is printing, and the printer is paused, the job stops printing and moves to the first position in the queue. When the printer is continued, this job prints first. If there is a pool of printer queues, this job is directed to the next available printer.

Examples

To pause all the shared printers at a server, type:

```
net admin \\acct.serve /c net pause print
```

where *acct.serve* is the name of the server; and all shared printers are paused.

To pause only the printer named *hplaser*, type:

```
net admin \\acct.serve /c net pause print=hplaser
```

where *acct.serve* is the name of the server, and *hplaser* is the printer's name whose services are paused.

To continue the *hplaser* printer, which was paused, type:

```
net admin \\acct.serve /c net continue
print=hplaser
```

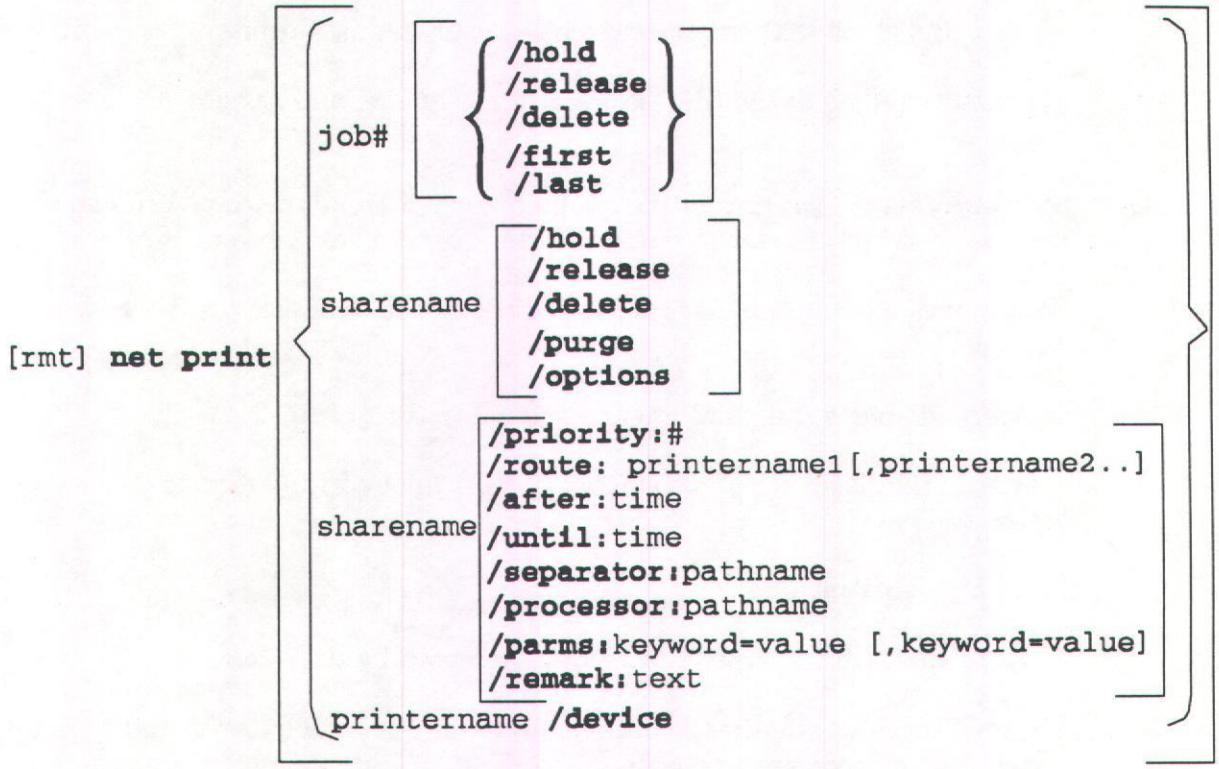
where *acct.serve* is the name of the server, and *hplaser* is the shared printer whose printing services are continued.

See Also

For information about	See
Sharing printer/printer queues	**net share**
Continuing paused services	**net continue**
What users can do using the **net pause** command	*Supermax LAN Manager/X - User's Guide*
Pausing resources on a server	*Supermax LAN Manager/X -System Administrator's Guide*
Stopping services on OS/2 clients	**net stop**

10.5.12. net print

Syntax



Purpose

This command displays and controls the contents of a shared printer queue.

Parameters

remote is required only when you are entering the command from the Enhanced DOS or OS/2 client system prompt. The *remote* parameter is replaced with:

```
net admin \\servername  /c
```

where *servername* is the name of the server you are administering.

job# specifies the identification number assigned to a print request in a queue.

sharename names the shared queue.

printername specifies the name of the printer being used.

after:*time* starts printing jobs from the queue after *time* (in 24-hour time, hh:mm, or in 12-hour time, hh:mm am or hh:mm pm). The server by default

checks the scheduled queues for start and stop times every ten minutes. To change the default time, you should modify the server's *lanman.ini* file by inserting or changing the **qsched=** keyword under the *lmxserver* section.

/delete deletes a specified job in a queue or deletes a specified queue.

/device indicates that the resource being modified is a printer.

/first moves a job to the first position in the queue, and assigns it a new job number.

/hold holds a job waiting in the queue to keep it from printing. You can also use the **/hold** parameter to hold a printer queue at the server.

/last moves a job to the last position in the queue, and assigns it a new job number.

/options displays the parameters assigned to the queue.

/parms: specifies a set of parameters for the queue in the format *keyword=value*.

Valid *keywords* include:

* **type** specifies the type of print data accepted by the queue.

* **eject** specifies whether a formfeed command is issued at the end of a print job. The choices are yes or no; the default is auto (yes).

* **copies** specifies number of copies to print. The default is 1.

* **banner** specifies whether to print a banner (separator) page before each job. The choices are **yes** and **no**; the default is **yes**.

/priority sets the priority to assign to the queue. (1 is the highest priority and 9 the lowest.)

/processor:*pathname* instructs the printer to use the print processing program stored in *pathname*.

/purge removes (purges) all jobs, except the current print job, from a queue.

/release releases a held job or printer queue.

/remark:*text* is a descriptive comment about the shared queue.

/route:*[printername1][,printername2...]* routes the printer ueue to one or more printernames on the server. Separate multiple printernames with semicolons (;) or commas (,).

/separator:*pathname* instructs the printer queue to use the separator page defined in the pathname file. You must specify the full path to the file. The default is no custom separator page; the UNIX lp subsystem banner page is printed instead (see the */parms* parameter).

/until:*time* prints jobs from the queue until time (in 24-hour time, hh:mm, or 12-hour time, hh:mm am or hh:mm pm). The server by default checks the scheduled queues for start and stop times every ten minutes.

When used without parameters, the **net print** command displays information about the server's printer queues, as follows:

```
Print Queues at    \\ACCT.SERVE
Name                Job#          Size      Status
POOL1 Queue         3 jobs                  *Queue Active*
   MARYJ              1           2509      Printing
   MARYJ              3             75      Waiting
   JOHNT              4             75      Waiting
LASER Queue         2 jobs                  *Queue Active*
   OLGAR              5            180      Printing
   MARYJ              6           2509      Spooling

The command completed successfully.
```

This screen displays:

Column	Contents
Name	Sharename of the printer queue and the name of the user who sent each job to the queue.
Job#	Identification number of each print job
Size	Size in bytes of each print job
Status	Status of each queue (including the number of jobs in it) or status of each print job (printing, paused, error, spooling)

Comments

The **net print** command allows you to do the following:

* list or modify the status of printer queues shared by the server
* list or modify parameters for printer queues shared by the server
* list or modify the status of print jobs in the queue



* display the contents of a printer queue

* control your print jobs in the queue

For information on the user's version of **net print**, see *Supermax LAN Manager/X - User's Guide.*

Working with Printer Queues
To find out about a specific printer queue on your server, include the sharename of the queue by typing a command in this form:

```
net admin \\acct.serve /c net print pool1
```

where *acct.serve* is the name of the server.

A display similar to the following appears:

```
Name            Job#      Size    Status
POOL1           Queue     Ø jobs  *Queue Active*

The command completed successfully.
```

To see current printing parameters for the queue, type the **net print** command with the */options* parameter as follows:

```
net admin \\acct.serve /c net print pool1 /options
```

where *acct.serve* is the name of the server.

A display similar to the following appears:

```
Printing Options for POOL1

Status              Queue Active
Remark              Spooled printers
Print Devices       hplaser, dde1080
Separator File      c:\usr\net\servers\lanman\spool\banner.net
Priority            8
Print After         12:00 AM
Print Until         11:59 PM
Processor
Parameters          COPIES=1 TYPES=Simple EJECT=AUTO BANNER=No

The command completed successfully.
```

To modify any of these printing parameters, use the **net print** command with the sharename of the printer queue and one or more of the following parameters:

To modify	Parameter
Remark	**/remark:**text
Print Devices	**/route:**[printername][;printername2...]
Separator File	**/separator:**pathname
Priority	**/priority:**number
Print After	**/after:**time
Print Until	**/until:**time
Processor	**/processor:**pathname
Parameters	**/parms:**keyword=value[;keyword=value2...]

A printer queue can be routed to a null device so that it is kept from printing, but not from accepting, jobs. To do this, use the */route* parameter but do not specify a printername. For example,

```
net admin \\acct.serve  /c net print sharename /route:
```

where *acct.serve* is the name of the server.

With the **net print** command, you can also purge or delete a queue shared by your server. When you use the **/delete** parameter to delete a queue, the following things happen:

* The queue does not accept any new print jobs; all users currently linked to the queue dropped
* The queue continues to print jobs already in the queue
* The queue is deleted when all jobs are printed

About Print Jobs

The server owning one or more printer queues assigns each print job a unique identification number. For example, if there is a job number 3 in one queue shared by a server, none of the other queues for that server will contain a job with identification number 3.

To get information about a particular print job on a remote server, the administrator specifies the job number. For example, you might type:

```
net admin \\acct.serve /c net print 35
```

where *acct.serve* is the name of the server.

A display similar to the following appears:

```
Job ID                35
Status                Waiting
Size                  3097
Remark
Submitting user       MARYJ
Notify                MARYJ
Job data type         dos
Job parameters        COPIES=1 EJECT=AUTO BANNER=No
Additional info

The command completed successfully.
```

The status of a print job may be:

* Waiting, Held in (queue's sharename)
* Printing on (devicename)
* Paused on (devicename)
* Error on (devicename)

Print jobs can be held or released with the **/hold** and **/release** parameters. Print jobs held in the queue stay in the queue until released. In the meantime, other printer jobs bypass the held jobs.

As administrator you can modify any user's print jobs or you can delete their print jobs from a printer queue with the **/delete** parameter.

You can use the **net print** command to change the position of a print job in a queue (with the **/first** or **/last** parameters).

Examples

A large file (identification number 263) is working its way through a printer queue on *acct.serve*. You know other people have shorter and more urgent print jobs waiting in the queue, so you decide to move the large print job to the end of the queue so that other jobs can print. After informing the user who wants to print the large file, you move it to the end of the queue by typing:

```
net admin \\acct.serve /c net print 263 /last
```

The person who wants to print the large file calls you back and asks you to hold off printing the file. You can hold the print job in the queue by typing:

```
net admin \\acct.serve /c net print 266 /hold
```



You will notice the job id has changed, since it has been moved to the end of the queue. Later that day, the person calls again and says to go ahead and print the file. You can release the file from the queue by typing:

```
net admin \\acct.serve /c net print 266 /release
```

You can also use the **net print** command to define a print schedule for an existing printer queue. For example, you may want to print all files over a specified size at night when the printers are not in use. The *laserprt* queue will print beginning at 8:00pm. To do this, type:

```
net admin \\acct.serve /c net print laserprt
/after:8.00pm
```

See Also

For information about	See
Sharing a printerqueue	**net share**
Creating separator pages	**net separator**
Checking the status of print devices	**net device**
What users can do with the **net print** command	*Supermax LAN Manager/X - User's Guide*
Creating and sharing printer queues, defining separator pages, and using the default Supermax LAN Manager/X print processor	*Supermax LAN Manager/X - System Administrator's Guide*

10.5.13. net save

Syntax

```
[remote]net save filename
```

Purpose

This command saves a copy of the current sharelist in a file on the server.

Parameters

remote is required only when you are entering the command from the Enhanced DOS or OS/2 client system prompt. The *remote* parameter is replaced with:

```
net admin  \\servername  /c
```

where *servername* is the name of the server you are administering.

For more information on using this parameter, see the *Administering Supermax LAN Manager/X via the Command Line Net Interface* section earlier in this chapter.

filename specifies the name assigned to the sharelist being saved. If you are executing the **net** save command from the **net** command shell, make sure the filename you specify does not already exist.

Comments

As administrator, you can use the **net save** command to make a copy of the current sharelist on a server. The sharelist is a binary file that contains a list of all available shared resources on a server. When you share a resource, it is automatically placed in the sharelist file. Use the **net load** command to load a previously saved sharelist that was created with the **net save** command to make this the new current sharelist. Use the **net save** command to retain a copy of the server's current sharelist for use at a later time.

Supermax LAN Manager/X places the file specified in the **net save** command into the */usr/net/servers/lanman/profiles* directory on the server and automatically adds the *.pro* extension to the filename. The **net save** command does not delete the current sharelist, it copies the contents of the list to another file.

Users can use the **net save** command to create profile (*.pro*) files for their clients. Profile files contain lists of **net use** commands that define a client's network connections. For more information on the user's version of the **net save** command, see *Supermax LAN Manager/X - User's Guide*.



Examples

Your department has two work shifts; each one needs access to a different set of resources on the same server. You must create two sharelists, one for each shift. Use the **net save** command to save a copy of the current sharelist for the day shift. Type:

```
net admin \\acct.serve /c net save daylist
```

where *acct.serve* is the name of the server; and *daylist* is the name of the file that contains the contents of the new sharelist file.

Now, modify the current sharelist for the night shift, adding and deleting shared resources as appropriate. See the **net share** command to add and delete shared resources.

To save a copy of the modified sharelist for the night shift, type:

```
net admin \\acct.serve /c net save nitelist
```

where *acct.serve* is the name of the server; and *nitelist* is the name of the file containing the modified contents of the current sharelist file.

To use *daylist* as your current sharelist file, use the **net load** command and type:

```
net admin \\acct.serve /c net load daylist
```

where *acct.serve* is the name of the server; and *daylist* is the name of the new sharelist file.

See Also

For information about	See
Loading an alternate sharelist on the server	**net load**
Using **net save** to create profile files on a client	*Supermax LAN Manager/X - User's Guide.*

10.5.14. net send

Syntax

```
remote] net send { alias { <filename } }
                 { *     { message  } }
                 { /users             }
```

Purpose

This commands sends messages and files to other users.

Parameters

remote is required only when you are entering the command from the Enhanced DOS or OS/2 client system prompt. The *remote* parameter is replaced with:

```
net admin  \\servername  /c
```

where *servername* is the name of the server you are administering.

For information on using this parameter, see the *Administering LAN Manager via the Command Line Net Interface* section earlier in this chapter.

alias specifies the username, groupname, or computername to which the message is to be sent. Groupnames can be specified only when administering a server running with user-level security.

When sending to a Basic DOS client the alias must specify the clients computername, not its username.

* indicates that all computers on the network are to receive a broadcast message.

/users sends the messages to all users currently connected to one of the server's resources.

<filename is the file sent as a message.

message specifies text sent as a message.

Comments

The **net send** command sends a short message to another user on the local area network. If the message is longer than one line, type the **net send** command, an alias, and press RETURN. You may include several lines, including carriage returns. When you have finished typing your message, press CTRL+Z to add an end of file character to your message. Press RETURN again to send the message.

If you use the * option to send a broadcast message, it is limited to 128 characters. When a message exceeds the maximum characters allowed, the excess characters are lost and the receiver is not notified that the message is incomplete.

Basic DOS and Enhanced DOS clients can receive files that are limited to 128 bytes; OS/2 clients can receive files that are limited to 62,000 bytes, but the OS/2 default buffer size is 4096 bytes. To increase the OS/2 message buffer, go to the client and adjust the **sizmessbuf=** parameter in the client's *lanman.ini* file or use the **net start messenger /sizmessbuf:#** command.

When you are sending a message to a user at an OS/2 client, the Messager service must be running on the intended receipient's computer. For DOS clients, the Message Receiver Program, *netmsg*, must be running on the intended receipient's computer. Your message is successfully received when the following message is displayed at your computer:

```
Message successfully sent to <name>.
```

If you use an unrecognized alias, or the Messenger service or the Message Receiver Program is not running on the intended receipient's computer, an error message is displayed.

Examples

To send a message to an alias called *annaj*, type:

```
net admin \\acct.serve /c net send annaj the
meeting is at 3 pm.
```

where *acct.serve* is the name of the server.

If you want to send a message to all users currently linked to the server about its impending shutdown, type:

```
net admin \\acct.serve /c net send /users server
coming down now.
```

where *acct.serve* is the name of the server.

See Also

For information about	See
User's version of **net send**	*Supermax LAN Manager/X - User's Guide*

10.5.15. net separator

Syntax

```
[remote] net separator { sharename { pathname | /delete } |
                         printername /device { pathname | /delete } }
```

Purpose

This command causes a custom separator page to print between each print job for a specified printer queue or printer.

Parameters

remote is required only when you are entering the command from the Enhanced DOS or OS/2 client system prompt. The *remote* parameter is replaced with:

```
net admin  \\servername  /c
```

where *servername* is the name of the server you are administering.

For information on using this parameter, see the *Administering Supermax LAN Manager/X via the Command Line Net Interface* section earlier in this chapter.

sharename specifies the sharename of the printer queue that is to use the separator page.

pathname specifies the pathname of the file containing the separator page description. Unless you specify otherwise, Supermax LAN Manager/X assumes pathname specifies a file in the */usr/net/servers/lanman/spool* directory.

printername specifies the name of a printer that is to use the separator page.

/delete cancels separator page printing for a printer queue. The default LP separator page is used. (See the */parms* parameter for the **net print** command for information on turning off the default for LP separator page.)

/device indicates that the resource being modified is a printer.

Comments

The **net separator** command can be abbreviated **net sep**.

A separator page typically includes the following information:

* the name of the client from which the print job was sent
* the filename of the print job
* the date and time the spool file was created

You can also use the **/separator** parameter with the **net print** command to assign a separator file to a printer queue. Separator pages are created on the UNIX operating system.

Examples

To start printing separator pages between print jobs on the printer queue *laserprt*, type:

```
net admin \\acct.serve /c net sep laserprt
banner.net
```

where *acct.serve* is the name of the server.

In this example, the *banner.net* file contains the actual text of the separator page.

To stop printing separator pages on printer queue *laserprt*, type:

```
net admin \\acct.serve /c net sep laserprt /delete
```

where *acct.serve* is the name of the server.

See Also

For information about	See
Administrating printer queues	**net print**
Separator pages	**net print**

10.5.16. net session

Syntax

```
[remote] net session { \\computername [/delete] }
                     { /delete                 }
```

Purpose

This command lists or disconnects sessions between the server and other computers on the local area network.

Parameters

remote is required only when you are entering the command from the Enhanced DOS or OS/2 client system prompt. The *remote* parameter is replaced with:

```
net admin  \\servername  /c
```

where *servername* is the name of the server you are administering.

For information on using this parameter, see the *Administering Supermax LAN Manager/X via the Command Line Net Interface* section earlier in this chapter.

computername lists the session information for a client.

/delete ends the session between the server and the client.

It also closes all open files associated with the session. If no computername is specified, it ends all sessions for the server.

When used without parameters, the **net session** command displays information about all user sessions on the server, as follows:

```
Computer        User name       Uses   Opens   Session time   Idle time
\\JTPC          JOHNT           1      1       12:37:43       12:37:31
\\MAJPC         MARYJ           1      1       00:13:56       00:00:41

The command completed successfully.
```

This screen displays:

Column	Contents
Computer	The computername associated with the session
Username	The username associated with the session

Uses	The number of shared resources being used with the session
Opens	The number of files opened by the session
Session time	The amount of time the session has existed
Idle time	The amount of time since there was activity between the server and the user's client during this session

Comments

This command can also be typed **net sessions** or **net sess**.

When used with the *computername* parameter, the **net session** command provides information about the session between the server and the specified computername, as follows:

```
User name          JOHNT
Computer           JTPC
Sess Time          00:13:59
Idle Time          00:00:44

Net name           Type          # opens
-------------------------------------------
LASER              Print
REPORTS            Disk           0

The command completed successfully.
```

Disconnecting and Reconnecting Sessions

You can specify how long a user's session can remain idle before Supermax LAN Manager/X automatically disconnects the session with the **autodisconnect=** parameter in your server's *lanman.ini* file. (A user may see that the session is disconnected when typing the **net use** command with the devicename parameter.)

If the user tries using the session after it is disconnected, the client tries to reconnect the session. If the username or password used to reconnect differ from that used to initially create the session, an error message is displayed.

Examples

To end a session between your server and a client, type the **net session** command as follows:

net admin \\acct.serve /c net session \\computername /delete

where *acct.serve* is the name of the server and *computername* is the name of the client to be disconnected.

To end all sessions between your server and other computers, type:

```
net admin \\acct.serve /c net session /delete
```

To display session information for the client annaj, type:

```
net admin \\acct.serve /c net session \\annaj
```

Looking at the resulting display, you realize that there is a problem associated with this session. Call Anna Jones to let her know that you must disconnect her session in order to correct the error. Then, to disconnect all sessions between annaj and the server, type:

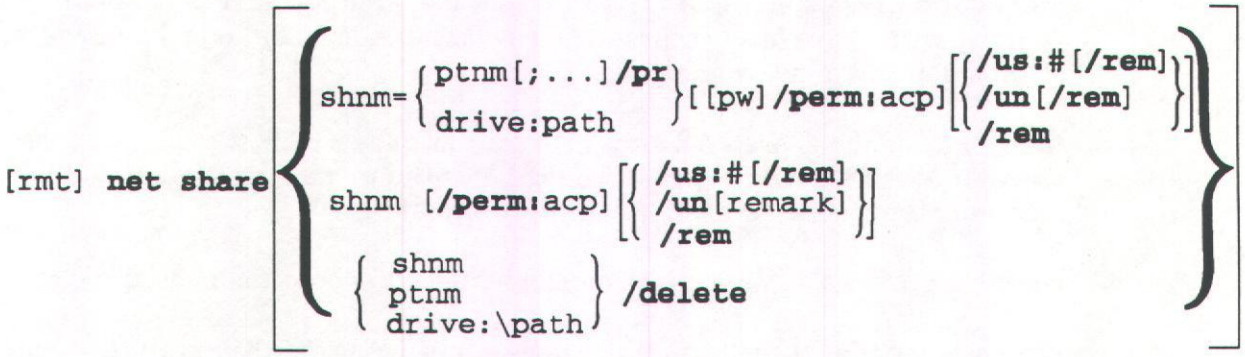
```
net admin \\acct.serve /c net session \\annaj /delete
```

See Also

For information about	See
Checking the status of sessions	**net status**

10.5.17. net share

Syntax



Purpose

This command makes a resource available to clients.

Before you can share a printer, configure your printer(s) on the UNIX system. For more information on using this parameter, see the *Administering Supermax LAN Manager/X via the Command Line Net Interface* section earlier in this chapter.

Parameters

rmt (remote) is required only when you are entering the command from the Enhanced DOS or OS/2 client system prompt. The *rmt* parameter is replaced with:

```
net admin  \\servername  /c
```

where *servername* is the name of the server you are administering.

For information on using the remote parameter, see the *Administering Supermax LAN Manager/X via the Command Line Net Interface* section earlier in this chapter.

ptnm[;...] specifies the printername(s) of one or more printers shared by sharename.

drive:path specifies a directory as the shared resource.

pw specifies the password required of users to use a resource shared by a server running with share-level security. Specify the password when you create the shared resource. The password cannot be more than eight characters.

shnm specifies the sharename of the resource being shared.

/delete stops sharing the resource.

/perm:acp assigns access permissions to the shared resource on a server running with share-level security. Access permissions (acp) may be any or all of the following: **r**, **w**, **c**, **x**, **d**, **a**, **p**.

/pr identifies the shared resource as a printer queue. This parameter must be specified when sharing a queue. You can use the **pr** abbreviation, any other unique abbreviation, or spell the entire word.

rem:*text* provides a descriptive comment (remark) about the shared resource.

/un specifies that there is an unlimited number of users that can use a shared resource simultaneously. If you use this parameter, auditing will be turned off for the shared resource. Unlimited is the default. You can use the **un** abbreviation, any other unique abbreviation, or spell the entire word.

/us:# specifies the maximum number of users that can use the shared resource simultaneously. You can use the **us** abbreviation, any other unique abbreviation, or spell the entire word.

When used without parameters, the **net share** command lists information about all resources being shared by the server, as follows:

```
Net Name   Device or Path                    Remark
------------------------------------------------------------------
ADMIN$     C:\USR\NET\SERVERS\LANMAN         Admin Share
IPC$                                         IPC Share
C$         C:\                               Root Share
UTIL       C:\USR\NET\SERVERS\LANMAN\UTIL    DOS Utilities
DDEADMIN   C:\USR\NET\SERVERS\DDEADMIN       DOS Utilities
BIN        C:\USR\LANMAN\DOSBIN              DOS Executables
USERS      C:\USR\LANMAN\USERS               Users home directory
PUBLIC     C:\USR\LANMAN\USERS\PUBLIC        Users public directory
DEP1       C:\USR\LANMAN\USERS\DEP1          DEP1 USER DIRECTORY
DEP2       C:\USR\LANMAN\USERS\DEP2          DEP2 USERS DIRECTORY
CANON      lmx                  Spooled      Printer in service division
DEP1P      print706             Spooled      Printer in dep 1
DEP2P      print708             Spooled      Printer in dep 2

The command completed successfully.
```

This screen displays:

Column	Contents
Net Name	The sharename of the resources being shared by the server

Device or Path	The printernames or pathnames being shared with the local area network
Remark	Descriptive comments about the shared resources

Comments

With Supermax LAN Manager/X, you can share the following resources from a server:

* Directories. To share the contents of a directory, use the **net share** command with a sharename plus the drive letter and path for that directory.

* Printer queues. To share a printer queue, use the **net share** command with a sharename and the printername associated with the printer served by the shared queue. You must also use the **/print** parameter to share a printer queue.

When used with just the *sharename* parameter, the **net share** command displays the following report:

```
Net Name                BIN
Pathname                C:\USR\LANMAN\DOSBIN
Remark                  DOS Executables
Permission
Max Uses                No limit
Uses                    MARYJ

The command completed successfully.
```

This report displays:

Column	Contents
Net Name	The sharename of the resource being shared
Pathname	The pathname of the resource being shared. If the resource is a printer queue, this field specifies the related printername.
Remark	The permissions assigned to the shared resource
Max Users	The maximum number of users who can use the shared resource at the same time
Users	The usernames of people currently using the resource.

Permissions

The permissions assigned to a shared resource with the **net share** command apply only when the server is running with share-level security. For information on assigning permissions when the server is operating in user-level security, see the **net access** reference page earlier in this chapter. Some permissions work only with specific types of resources, as follows:

Code	Permission
r	"read" lets users read a directory's file or copy its files to other directories. It also lets users view the names of files in a shared directory. When used by itself, it allows users to look at or execute programs only.
w	"write" lets users make changes to the files in a directory. In most cases, it should be used in combination with read permission.
c	"create" lets users create files and subdirectories in a shared directory. When used by itself, it lets users create new files in the directory and change them while they are creating them. Once the file is closed, it cannot be modified.
x	"execute" lets users run a command or program.
d	"delete" allows users to delete files and subdirectories.
a	"change attributes" lets users change file attributes. For more information on file attributes, see your DOS or OS/2 documentation.

Examples

After you have configured your printer(s) on the UNIX system, you can share a printer queue. Type:

```
net admin \\acct.serve /c net share
laserprt=hplaser /print
```

where *acct.serve* is the name of the server; *laserprt* is the name of the shared printer queue; and *hplaser* is the name of the printer.

To share the two printers with the UNIX lp subsystem printernames *hplaser* and *dde1080* as a printer pool served by a single printer queue, type:

```
net admin \\acct.serve /c net share
pool1=hplaser;dde1080 /print
```

where *acct.serve* is the name of the server; *pool1* is the name of the printer pool served by the shared printer queue; and *hplaser* and *dde1080* are printer names.

Now that the printer queues are shared, assign access permissions to these resources. For servers running with share-level security, permissions are assigned to the shared resource. For example, to assign access permissions to a shared printer queue, type:

```
net admin \\acct.serve /c net share laserprt
/perm:y
```

where *acct.serve* is the name of the server; *laserprt* is the name of the shared printer queue; and **y** represents the word yes allowing users to submit files to the printer queue.

For servers running with user-level security, assign access permissions for users to a printer queue that has not previously been assigned permissions for other users by typing:

```
net admin \\acct.serve /c net access
\print\laserprt /add annaj:y
```

where *acct.serve* is the name of the server; **\print** specifies that *laserprt* is the shared printer queue; *annaj* is the first user to have access permissions to submit files or requests to *laserprt*.

There are two ways to create new directories:

1. To create a new directory on the UNIX operating system, log on to the server console as *root*. Change from the current directory, if you do not want the new directory to be in root's home directory.

   At the prompt type:

   mkdir <directory name>

   and press RETURN.

   Change the permissions, ownership, and group for this directory to agree with Supermax LAN Manager/X permissions, ownership, and group. At the prompt type:



```
chmod 775 <directory name>

chown lmxadmin <directory name>

chgrp DOS---- <directory name>
```

and press RETURN.

2. To create a new directory at the client, log on as a user with administrative privileges. Link to *C$* and change directories to the path specified in the *userpath=* parameter in the server's *lanman.ini* file. The specified default is */usr/lanman*. Then type:

```
mkdir <directory name>
```

and press RETURN.

To share a directory and assign a password to this share directory, type the **net share** command as follows:

net admin \\acct.serve /c net share sharedir**=c:\usr hello**

where *acct.serve* is the name of the server; *sharedir* is the name of the shared resource; *c:\usr* is the full path that links to sharedir; and *hello* is the password assigned to sharedir.

Assign access permissions to the shared resource on servers running share-level security by typing:

net admin \acct.serve /c net share sharedir **/perm:rwcxd**

where *acct.serve* is the name of the server; *sharedir* is the name of the shared resource; **rwcxd** represent read, write, create, execute, and delete permissions assigned to *sharedir*.

To assign access permissions for a user to a shared resource that has not previously been assigned permissions for other users on a server running user-level security, type:

```
net admin \acct.serve /c net access e:\sharedir /add
annaj:rw
```

where *acct.serve* is the name of the server; *e:* is the drive linking to *sharedir*; and *annaj* is the user assigned read and write permissions on *sharedir*.

To stop sharing a resource, type:

```
net admin \\acct.serve  /c net share sharedir
/delete
```

where *acct.serve* is the name of the server; and *sharedir* is the name of the discontinued shared resource.

See Also

For information about	See
Assigning permissions to resources on user-level servers	**net access**
Defining, controlling, and deleting printer queues	**net print**
Using shared resources	*Supermax LAN Manager/X - User's Guide.*
Sharing resources and administrating shared resources	*Supermax LAN Manager/X - System Administrator's Guide*

10.5.18. net statistics

Syntax

```
[remote] net statistics { /clear }
                        { server  }
```

Purpose

This command displays and clears a server's list of usage statistics.

Parameters

remote is required only when you are entering the command from the Enhanced DOS or OS/2 client system prompt. The *remote* parameter is replaced with:

```
net admin  \\servername  /c
```

where *servername* is the name of the server you are administering.

For information on using this parameter, see the *Administering Supermax LAN Manager/X via the Command Line Net Interface* section earlier in this chapter.

/clear clears the statistics log.

server specifies the Server service.

Comments

This command can also be typed **net stats**.

When you type the **net statistics** command with the **server** parameter, it displays statistics about the server, as follows:

```
Network Statistics for \\acct.serve

Statistics since OCT 27, 1987, 13:12:23

Sessions accepted                1  Bytes received (KBytes)          503
Sessions timed out               0  Bytes sent (KBytes)             1225
Sessions errored out             0  Mean response time (msec)          0

Network errors                   2  Network I/O's performed           43
System errors                    0  Files accessed                     1
Password violations              0  COM devices accessed               0
Permissions violations           0  Print jobs spooled                 0

The command completed successfully.
```

This screen displays:

* the date on which the statistics log was last cleared
* the number of sessions accepted, disconnected automatically, and disconnected by an error
* the number of bytes sent and received, along with the average server response time
* the number of errors and violations of passwords and permissions
* the number of times shared files, and printers were used

Example

To display a list of statistics for your server, type:

```
net admin \\acct.serve  /c net statistics server
```

where *acct.serve* is the name of the server.

See Also

For information about	See
Collecting and displaying usage information	**net audit**
Displaying the contents of the server's error log	**net error** and Chapter 2 of this guide

10.5.19. net status

Syntax

```
[remote] net status
```

Purpose

This command displays a server's computername, configuration settings, and a list of shared resources on the server.

Parameters

remote is required only when you are entering the command from the Enhanced DOS or OS/2 client system prompt. The *remote* parameter is replaced with:

```
net admin  \\servername  /c
```

where *servername* is the name of the server you are administering.

For information on using this parameter, see the *Administering Supermax LAN Manager/X via the Command Line Net Interface* section earlier in this chapter.

Comments

There are no parameters for this command.

The **net status** command displays the same information as the **net config** and **net share** commands combined.

Example

To see the configuration values and shared resources for *acct.serve*, type:

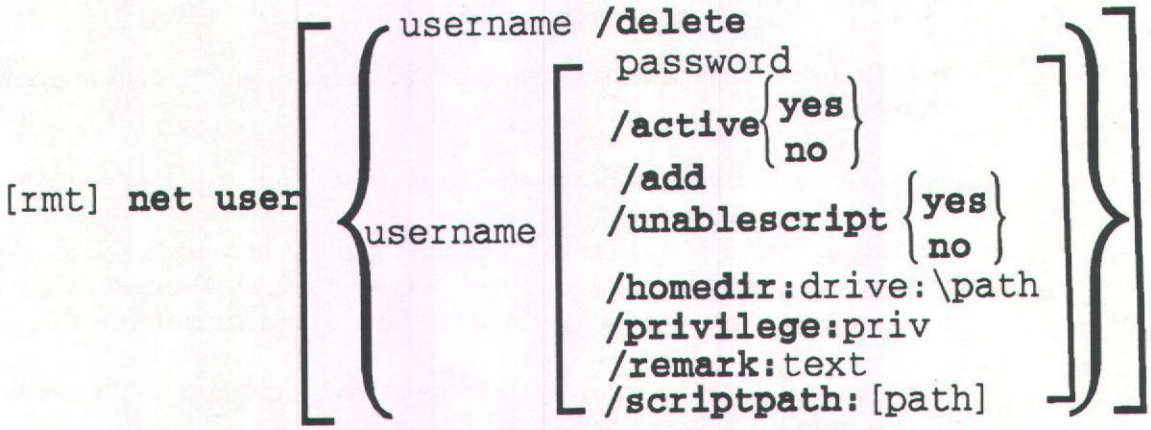
```
net admin \\acct.serve /c net status
```

See Also

For information about	See
Displaying server configuration	**net config**
Displaying the resources being shared from a server	**net share**
Displaying a list of server usage statistics	**net statistics**
Displaying a list of shared resource usage information	**net audit**

10.5.20. net user

Syntax



Purpose

This command lists, adds, removes, and modifies user accounts on the server. It is available only on servers running with user-level security.

Parameters

remote is required only when you are entering the command from the Enhanced DOS or OS/2 client system prompt. The *remote* parameter is replaced with:

```
net admin  \\servername  /c
```

where *servername* is the name of the server you are administering.

For more information on using this parameter, see the *Administering Supermax LAN Manager/X via the Command Line Net Interface* section earlier in this chapter.

username specifies the username, up to 20 characters, for the account to be added, deleted, or modified.

password specifies the password, up to 14 characters, to be assigned to username.

/active:[yes|no] specifies whether or not this is an active account. If the account is not active, the user cannot access the server. (The default is **yes**.)

/add adds a user account to the server.

/delete deletes a user's account from the server.

/enablescript:[**yes** | **no**] specifies whether or not a script is to be used as part of this user's logon verification process if logon security is being used. (The default is **yes**.)

/homedir:drive:\path specifies the pathname of the user's home directory.

/privilege:*priv* specifies the user's privilege level, where *priv* is **guest**, **user**, or **admin**.

/remark:*text* provides a descriptive comment about the user's account.

/scriptpath:*path* identifies the location of this user's logon script, if one is to be used. (Unless otherwise specified, Supermax LAN Manager/X assumes path is relative to the userpath specified in the server's *lanman.ini.* file.)

When used without parameters, the **net user** command displays the names of all user accounts on the server, as follows:

```
User Accounts for \\acct.serve
-------------------------------------------------------------------------------
JOHNT        GUEST        JENNYT
MARYJ        OLGAR

The command completed successfully.
```

Comments

This command can also be typed **net users**. It works only with servers operating with user-level security.

When used with the *username* parameter, the **net user** command displays information about an individual user account, as follows:

```
User name                    MARYJ
Privilege level              USER
Account active          Yes
Home directory          C:\LANMAN\USER\MARYJ
Password date                Wed Oct 14 16:02:32 1987

User comment            Mary Jones
Logon script path            SCRIPTS\NETLOGON.CMD
Logon script state           Disabled
Group memberships            *USERS       *UEXEC
                     *ADM

The command completed successfully.
```

This screen displays:

Column	Contents
User Name	The name of the account for this user
Privilege level	The privilege level associated with the username (guest, user, or admin)
Account active	Whether or not this is an active account
Home directory	The location of this user's home directory on the logon server
Password date	The date the account's password was last changed
User comment	The remark associated with the username
Logon script path	Where the user's logon script resides, if one exists
Logon script state	Whether a logon script is currently being used for this account
Group memberships	The groupnames of all groups to which the username belongs

Before you can specify a home directory for a user, that directory must exist on the server. You must also assign access permissions for that directory using the **net access** command. The **net user** command will not create a user's home directory automatically.

When you assign user or admin privilege to a user's account, that user is automatically included in the users group. A user whose account is assigned the guest privilege is not included in the users group.

Admin privilege grants the user of the account full access to all server resources and remote administration capability.

The **/active:no** parameter is used to temporarily suspend the privileges of a user's account.

When you create a new user account, decide if the user will have a home directory on the UNIX system. For more information on creating home directories on the UNIX system, see the *Supermax LAN Manager/X - System Administrator's Guide*

Examples

To set up a new user account for Mary Jones that will give her administrative privileges, type:

```
net admin \\acct.serve /c net user maryj adm /add /priv:admin
```

where *acct.serve* is the name of the server; *maryj* is the username of the newly created account; *adm* is the password for this account; and *admin* gives the username annaj administrative privileges.

To change this user's password to *smith* and revoke her administrative privilege, type:

```
net admin \\acct.serve /c net user maryj smith /privilege:user
```

where *acct.serve* is the name of the server; *smith* is the new password; *user* gives the username *maryj* user privileges.

Now that you have created a new user, assign access permissions for this user to shared resources. To assign access permissions for a user to a shared resource on a server running with user-level security, type:

```
net admin \\acct.serve /c net access c:\usr /add maryj:rw
```

where *acct.serve* is the name of the server; *c:\usr* is the full path that links to *sharedir*; and *maryj:rw* gives the username *maryj* read and write permissions on sharedir.

Users can also belong to groups. To assign a user(s) to an existing group, type:

```
net admin \\acct.serve /c net group sales maryj johnt /add
```

where *acct.serve* is the name of the server; *sales* is the name of the group; and *maryj* and *johnt* are the usernames to be added to the group called sales.

See Also

For information about	See
Assigning permissions for user accounts	**net access**
Working with groups of users	**net group**
Creating and administering user accounts, using centralized logon validation, and assigning access permissions for resources	*Supermax LAN Manager/X - System Administrator's Guide*

Appendix A. Managing Share-Level Security

This appendix describes and compares the Server Program's share-level and user-level security modes. It also describes how to set up a server to run the share-level security mode. Share-level security controls access on a per-resource basis, rather than on a per-user basis (as with user-level security).

For definitions of the two resource security modes, see Chapter 2, *Understanding the Server Program*. For information on setting up a server to run the user-level security mode, see Chapter 4, *Setting Up a User-Level Security Server*.

Important: Both the Audit Trail (resource auditing) and logon validation are not available on servers running share-level security.

A1. What Is Share-Level Security?

Using share-level security, you assign a password and a single set of access permissions to each resource shared on a server. Any user knowing the password can use that resource, within the limits of the resource's access permissions.

A1.1. Passwords

Under user-level security, a user needs to know only one password in order to access resources on a server; that password is part of his or her user account. Once the server verifies the password, it will not ask for it again.

Under share-level security, a user may have to supply a different password for each resource. Share-level security servers do not maintain user accounts. You cannot change a password without deleting the sharename and re-establishing it with a different password.

Running either security mode, users must provide a username and password when they log on to the LAN. However, if the server is running user-level security, additional passwords are not required to access a server resource. If the server is running share-level security, users may be prompted for a number of different passwords, according to the various resources being accessed.

In both security modes, users issue the same commands to request access to the server, and the server responds to them in the same way.

A1.2. Access Permissions

Under share-level security, when you share a resource you assign a set of access permissions for that resource. Share level security grants that same set of access permissions to each user who knows the password for the resource. The meaning of most of the disk resource access permissions (*RWCDX*) is the same as for user-level security. There are certain differences, however. Under share-level security:



* All users have the same set of access permissions for a shared resource. However, you can share the same resource multiple times, with different sharenames. For each sharename, you can specify a unique password and set of permissions. Users who access the resource by using one sharename and password can have different access permissions than users accessing the same resource by using another sharename and password.

* The **P** access permission, which means *Change access permissions* in user-level security, means **administrators** only in share-level security. See the following section for more information on administration and the **P** access permission.

A1.3. Access to Resources Under Share-Level Security

The method used by a server running share-level security to determine whether or not a user should be allowed to use a shared resource is illustrated in Figure A-1. Basically, a user's ability to access and perform operations with a shared resource depends upon three general considerations:

1. Is the **P** access permission set for this resource? If not, then continue to the next check. The **P** access permission (*administrators only* in share-level security) overrides all other access permissions and passwords.

2. Does the user's password match the resource's? If so, then continue to the next check. If not, prompt once for a different password. If this password does not match, deny access to the resource.

3. Do the share access permissions allow the requested activity? if so, grant the request. If not, deny access to the resource.

A1.4. Administrative Differences

Under user-level security, an administrator is any user account with the admin privilege level. Share-level security, however, does not recognize the concept of user privilege levels. Under share-level security, an administrator is anyone who is linked to the *ADMIN$* special administrative shared resource.

If you want to administer a share-level server, when you first log on to the network, use the username admin and enter the *ADMIN$* resource password at the *Password:* prompt. The first time you use a **net** command, you will be linked automatically to the *ADMIN$* resource.

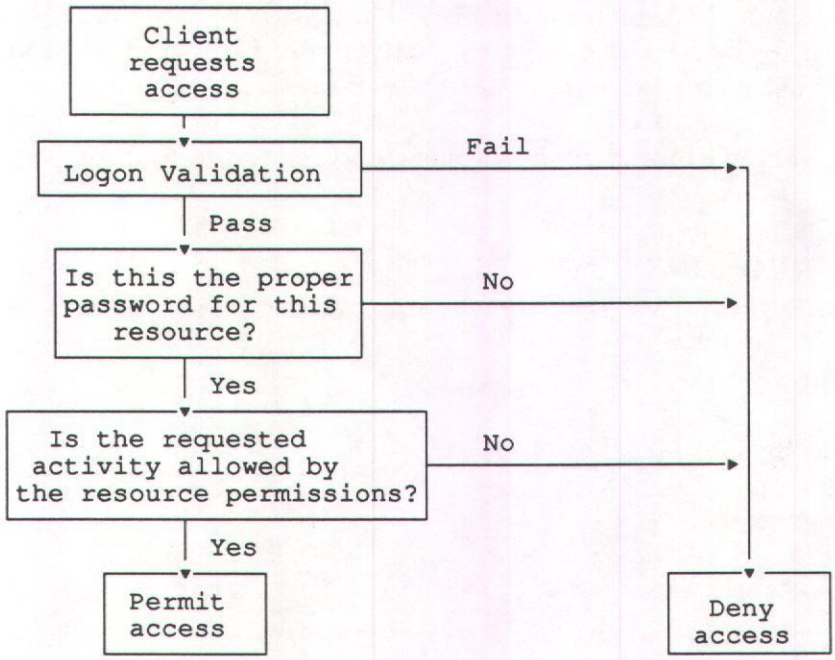
If you do not use this username and password, you will have to manually link to the server's *ADMIN$* resource before you can perform administrative functions. For example, if the *mis.serve* server's ADMIN resource password is *pass1*, then you could get administrative privileges on the *mis.serve* server by typing the following command:

```
net use d: \\mis.serve\admin$ pass1
```

Do not share the *ADMIN$* resource without a password, since this would allow any user to be an administrator on the server.

On a share-level security server, an administrator can

* Use resources that have the **P** access permission.
* Issue LAN Manager administrative commands to the server.



Figur A-1. Access Under Share-Level Security

A1.5. Sharing Resources

For each resource that you share, you may define a password and a set of access permissions. For a user to be able to access the resource, the following conditions must be met:

* The user must know the password for the resource, if you have set one.
* The action that the user wants to take must be allowed by the assigned access permissions.

A1.6. Sharing the Special Administrative Resources

Under share-level security, the Server Program sets up some special shared resources every time you start the server. The sharenames of these resources end in a dollar sign (*$*), identifying them as special administrative resources. You cannot delete these resources.

Two resources require special handling under share-level security:

* *IPC$* is for interprocess communication (IPC). With this shared resource, users can look at (view) the resources on the server.

  Caution: Do not password protect the *IPC$* resource.

* *ADMIN$* is for server administration.

  Caution: Do not assign the **P** access permission to the *ADMIN$* resource. If the **P** permission is assigned to the *ADMIN$* resource, you will not be able to link to the resource and you will not be able to administer the server.

To plan and configure a server running share-level security, continue to the next section, *Setting Up Share-Level Security.*

A2. Setting Up Share-Level Security

To set up a server running share-level security, you must perform the following tasks:

1. Plan the server setup
2. Configure the server for share-level security
3. Start the Client Program
4. Log on as the administrator
5. Share directories
6. Set up shared print queues

Figure A-2 illustrates the set up tasks, presented in the order in which they should be performed.

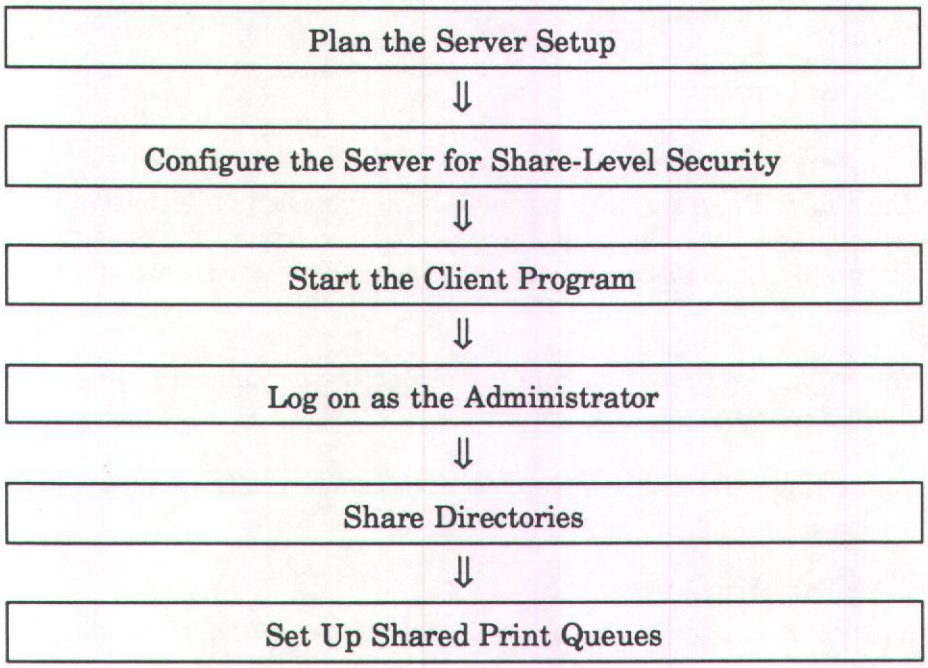


Figure A-2. Setting Up a Server With Share-Level Security

A2.1. Planning the Server Setup

To plan for a server running share-level security, you must know:

* How many users will have access to this server

* What resources (disk and printer) will users require

* What directories and files should be available to some users but not to others

Because share-level security does not include the concepts of users or groups, the password is the primary means for controlling access to resources.

For example, to restrict access to a particular directory or printer, assign a password to the directory and distribute the password only among users will be permitted access. To grant access to all users, share the directory and assign no password. By sharing the same directory under multiple sharenames and passwords, you can also grant different users different access permissions for the same resource, allowing some read-only permissions, while others might have read-write access permissions.

A2.2. Configuring the Server for Share-Level Security

The Server Program operates in the user-level resource security mode by default. To configure your server for share-level security, you must change the value of the *security=* parameter under the *[server]* section of the server's *lanman.ini* file.

Change the parameter value with a text editor. Instructions for doing this appears in the section entitled *Changing Parameter Values With a Text Editor* in Chapter 9, *Changing the Default Server Configuration*.

A2.3. Starting the Client Program

Before you can start the Client Program, it must have been installed on either your computer's hard disk or a Client Boot Diskette. (For complete information concerning installing the Client Program, see *Supermax LAN Manager/X - Client Installation Guide*.)

Note: To administer the server, you must be running either the Enhanced DOS or the OS/2 version of the Client Program.

To start the Client Program, see the *Supermax LAN Manager/X - User's Guide* (Chapter 5).

A2.4. Logging On As the Administrator

After starting the Client Program, you must log on to the server you want to administer. When you log on, you must link to the *ADMIN$* resource on the server.

To log on to a server as an administrator, follow the instructions in the section entitled *Accessing the Full Screen Net Admin Interface*, in Chapter 3. Be sure to supply the password for the *ADMIN$* resource when you log on.

Example
You want to perform some administrative tasks on the *print2.serve* server down the hall. Rather than walk to the *print2.serve* server, you decide to administer the server from your client. Because you are not logged on as the administrator on the *print2.serve* server, you must log on to that server as *ADMIN*.

You log on to the network by typing **net logon ADMIN** `password` at the client's system prompt (replacing *password* with the appropriate password for the *ADMIN$* resource). Then you press RETURN.

You invoke the Full Screen Net Admin Interface and identify *print2.serve* as the server you intend to administer by typing `net admin \\print2.serve` and pressing RETURN. The *Administering* display field of the Full Screen Net Admin Interface shows the *print2.serve* servername. This verifies that you are now administering the *print2.serve* server.

A2.4.1. Equivalent net Command

You can also administer a server by using the **net admin** command. For more information about the **net admin** command, see Chapter 10, *Command Directory*.

A2.5. Sharing Directories

To share a directory on a server running share-level security, follow these steps:

1. Start the Full Screen Net Admin Interface and access the server you wish to administer. (For instructions, see the section entitled *Accessing the Full Screen Net Admin Interface*, in Chapter 3.)

2. Select the *View* menu and select the *This server* menu item.

   The *Resources This Server is Sharing With the Network* dialog box appears. This dialog box displays all resources currently being shared from the server (at this point in the set up process, the only shared resources to appear should be the default shared directories).

3. Select the *Add share* command button.

   The *What would you like to share?* dialog box appears.

4. Select the *Disk directory* option button.

   The *Share a Disk Resource With the Network* dialog box appears. (Figure A-3).

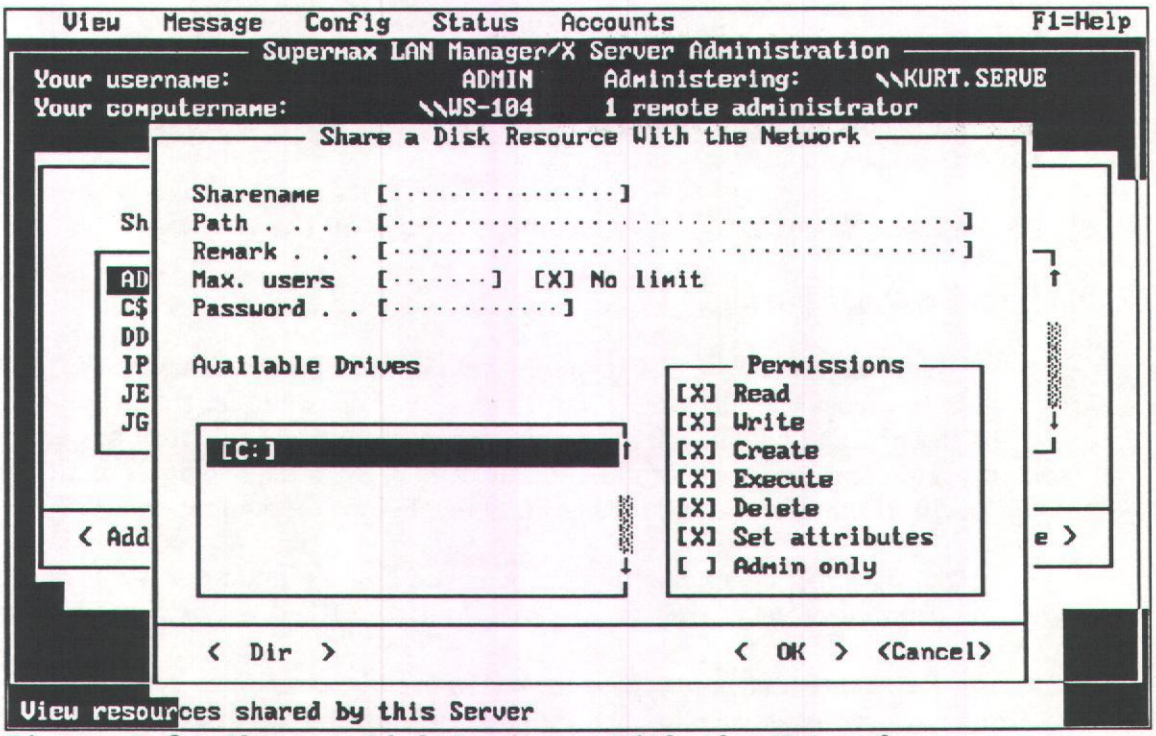


Figure A-3. *Share a Disk Resource With the Network*

Enter information into the text boxes of the *Share a Disk Resource With the Network* dialog box as follows:

a) At the *Sharename* text box, type the sharename for the directory being shared. This is the shared resource name that users will link to when they need to access the directory's contents.

   Sharenames for directories can be a maximum of 8 alphanumeric characters.

b) At the *Path* text box, type the drive letter and path of the server directory you are sharing.

   The format of the path statement is as follows:

```
driveid:\directory\subdirectory
```

   Where *driveid* is the drive (usually C: for the server's hard disk) where the shared directory is stored; and *\directory\subdirectory* is the UNIX system pathname for the shared directory (note the use of backslashes between directory names).

   If you specify a path that contains a directory that does not exist, LAN Mana ger will attempt to create that directory. In such cases, you should specify a path that starts with the default administerable LAN Manager directories (such as the *c:\usr\lanman* or *c:\usr2\lanman* directories). For more information about specifying the proper path, refer to the section entitled *Recommended Locations for Creating New Shared Directories*, in Chapter 4, *Setting Up a User-Level Security Server*.

c) At the *Remark* text box, type a comment describing the directory.

d) Do *one* of the following:

   * At the *Max. users* text box, type the maximum number of users that will be able to access the directory simultaneously. For example, this number may be determined by the software license agreement of a network application program that will be stored in the directory. Such license agreements can specify the maximum allowable number of simultaneous users.

   * At the *No limit* check box, mark the check box if you do not wish to limit the number of users that will be able to access the directory simultaneously.

e) At the *Password* text box, type a password for the directory. On servers running share-level security, the maximum allowable length for a password is 8 alphanumeric characters. The minimum allowable length for a password is determined by the value of the *minpassword=* parameter in the *[lmxserver]* section of the server's *lanman.ini* file (for more information about this parameter, see Chapter 9, *Changing the Default Server Configuration*).

6. Move to the *Permissions* check boxes. Use these boxes to assign access permissions for the directory.

7 Select the *OK* command button.

A2.5.1. Equivalent net Command

You can also share directories and assign access permissions with the **net share** command. For more information about the **net share** command, see Chapter 10, *Command Directory*.

A2.6. Setting Up Shared Print Queues

Before sharing a printer that is connected to the server you must configure the UNIX system for this printer. To configure the printer port, see Chapter 7, *Lp Spooler Administration*, in the *Supermax System V - System Administrator's Guide*. Confirm that the printer is set up correctly by printing from the UNIX system.

Then, to share a printer that is connected to the server, see Chapter 4, *Sharing Print Queues*.

A2.7. Managing Resources

A resource is anything you can share using the Server Program. Resources are shared print queues, disk drives, directories, and files provided by the server.

This section describes how to:

* Look at passwords and access permissions
* Change access permissions
* Change passwords
* Assign remote UNIX system process execution privileges

A2.7.1. Looking at Passwords and Access Permissions

When you share resources under share-level security, you must assign a password and a set of access permissions to each resource. You may need to check the passwords or access permissions under the following circumstances:

* When someone who should have access to a resource can't use it
* When you have forgotten the passwords or access permissions for a resource
* When you want to change a password or the access permissions for a resource

To look at the password and access permissions for a resource, follow these steps:

1. Start the Full Screen Net Admin Interface and access the server you wish to administer. (For instructions, see the section entitled *Accessing the Full Screen Net Admin Interface*, in Chapter 3.)

2. From the *View* menu, select the *This server* menu item.

   The *Resources This Server Is Sharing With the Network* dialog box appears. (Figure A-4).

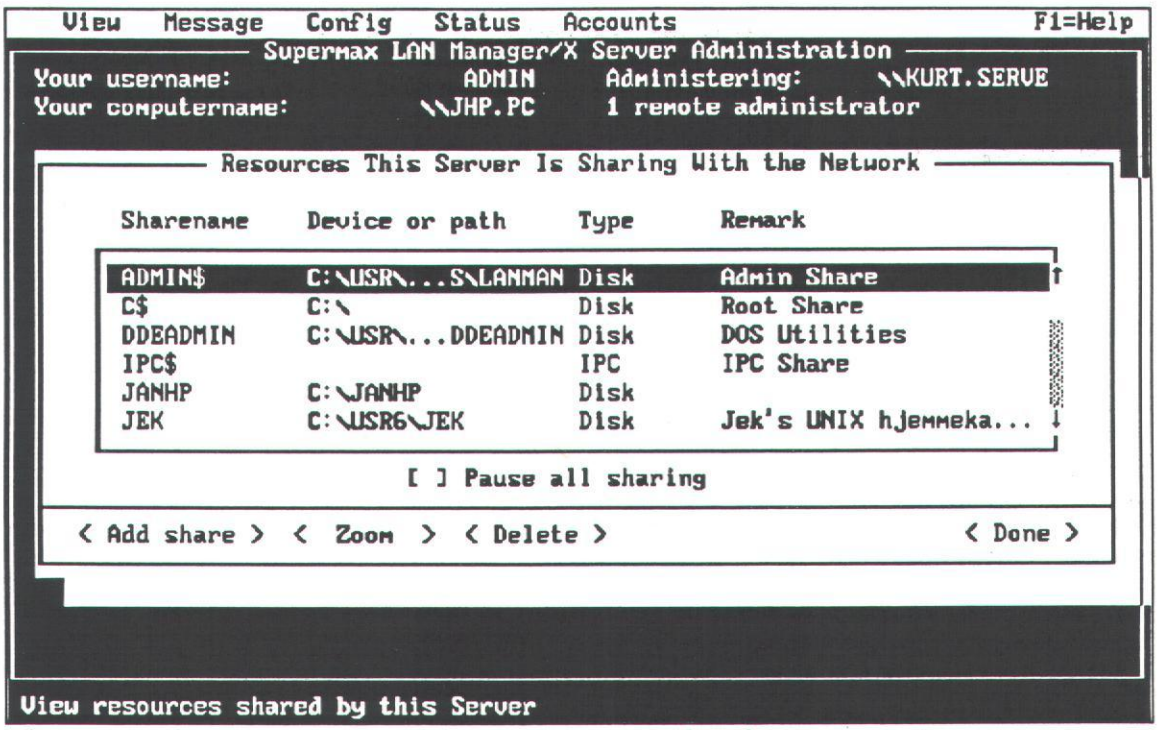


Figure A-4. *Resources This Server Is Sharing...*

3. Highlight the resource you want to examine in the list box.

4. Select the *Zoom* command button.

   The *Shared Resource Information* dialog box appears. (Figure A-5).

   The password for this shared resource is in the *Password* display field. The access permissions are in the *Permissions* display field.

If the *Password* display field is empty, then there is no password on this resource. Access to this resource is determined as follows:

* If the **P** access permission is set, only administrators can access the resource.

* If the **P** access permission is not set, anyone can access the resource (subject to the other access permissions).

If the password and access permissions appear to be correct but access is still denied, the UNIX system permissions may be in conflict with Server Program access permis-

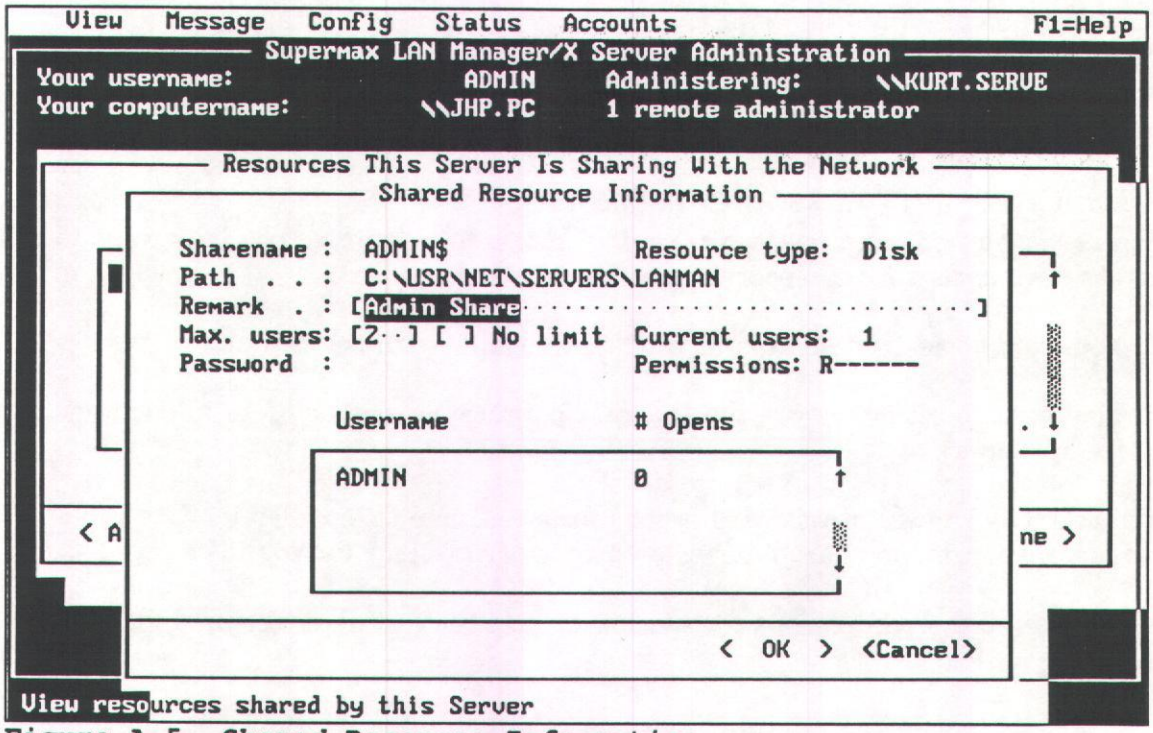


Figure A-5. ***Shared Resource Information***

sions. For more information, see the *Supermax LAN Manager/X Troubleshooting and Command Reference*.

Example

You are the administrator for the *print2.serve* server, a server running share-level security. The *print2.serve* server shares six printers and several directories with the LAN.

A user tells you she is unable to write a file to the *print2**scratch* directory (a large shared directory intended for general-purpose use). You suspect that you forgot to include the **W** access permission when you shared the directory.

You log on as the administrator and use the Full Screen Net Admin Interface to access the *print2.serve* server, using the instructions in the section of this appendix entitled, *Logging On As the Administrator*.

You select the *View* menu and then select the *This server* menu item. In the *Resources This Server Is Sharing With the Network* dialog box, you select the *scratch* directory and select the *Zoom* command button.

In the *Shared Resource Information* dialog box, you see that the access permission set for the *scratch* directory is *RCDAX*; you did indeed forget to specify **W** access permission.

A2.7.2. Equivalent net Command

You may also look at a resource's access permissions by using the **net share** command. For more information about the **net share** command, see Chapter 10, *Command Directory*.

A2.8. Changing Access Permissions

Access permissions and passwords control access to resources. You may want to change access permissions for a resource when:

* You want to restrict or expand what users cando with the resource
* You want to set or remove the **P** access permission, closing off or allowing access to the resource

You can only change access permissions for a resource that is being shared. If a resource is not being shared, it has no access permissions for you to change.

To change access permissions for a resource, use the **net share** command with the following options:

```
net admin \\server.serve /c net share sharename perm:permissions
```

where

* *server* is replaced with the name of the server being administered
* *sharename* is replaced with the name of the shared resource
* *perm:* tells the Server Program to change access permissions to those specified by *permissions*
* *permissions* specifies the access permission set for this resource (any combination of *RWCDXAP*)

An alternative method for changing a resource's access permissions is to delete the sharename and re-share it with the correct access permissions, using the Full Screen Net Admin Interface.

A2.8.1. Changing Passwords

Passwords and access permissions control access to resources. You may need to change a password for security reasons.

To change the password for a resource, you must stop sharing the resource and then reshare it with a new password. You cannot change the password when the resource is being shared.

To change the password for a shared resource, follow these steps:

1. Using the procedure in the section of this appendix entitled, *Looking at Passwords and Access Permissions*, make a note of the current password and access permissions for the shared resource that you want to change.

2. Select the *View* menu and select the *This server* menu item.

   Make sure that the name of the server you wish to administer is displayed in the *Administering:* display field of the background screen.

3. In the *Resources This Server Is Sharing With the Network* dialog box, highlight the resource you want to change in the list box.

4. Select the *Delete* command button.

   The *Stop Sharing a Network Resource* dialog box appears. (Figure A-6).

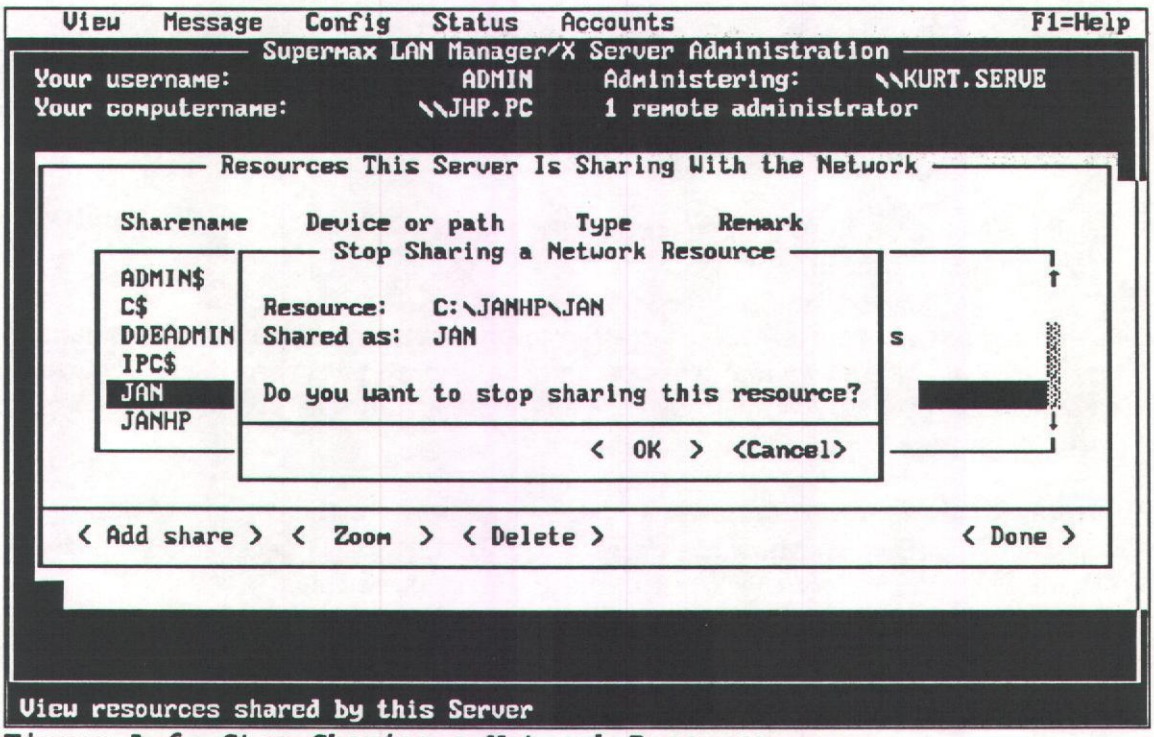


Figure A-6. *Stop Sharing a Network Resource*

5. Select the *OK* command button to delete the shared resource.

   The *Resources This Server Is Sharing With the Network* reappears.

6. Select the *Add share* command button.

   The *What would you like to share?* dialog box appears. (Figure A-7).

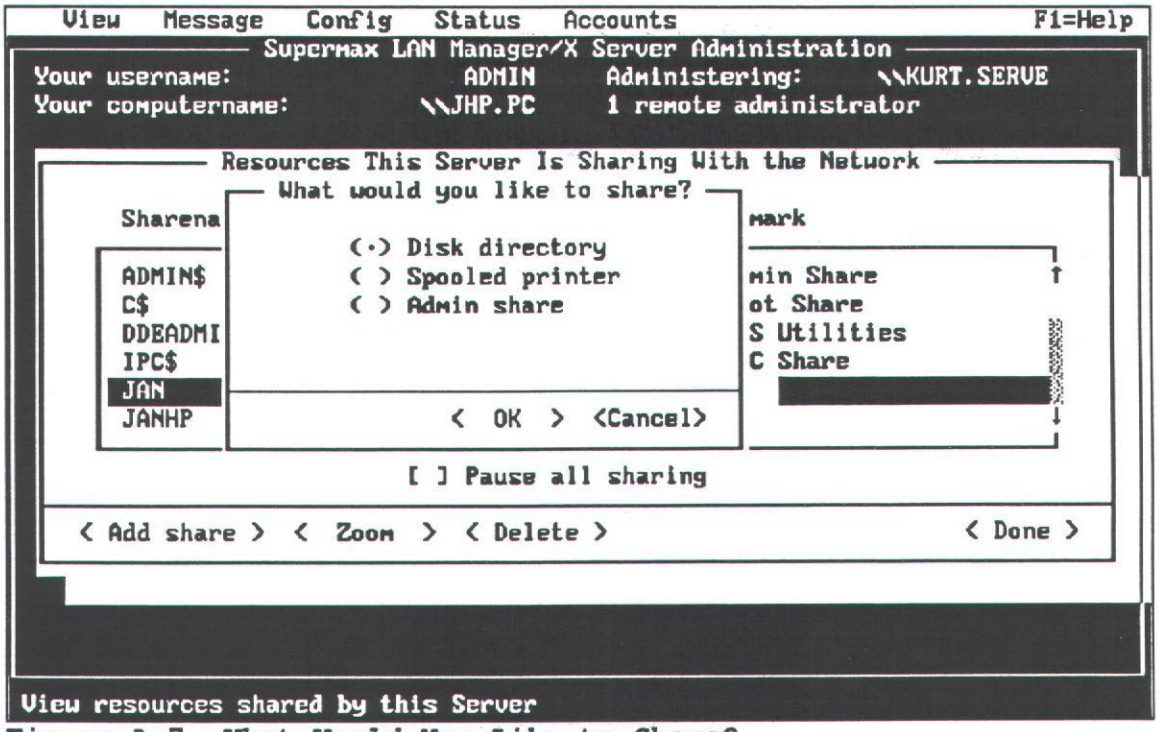


Figure A-7. *What Would You Like to Share?*

7. Select the option button for the type of resource you want to share and select the *OK* command button.

   A dialog box appropriate to that resource type appears. Type the sharename for the resource in the *Sharename* text box and the desired password in the *Password* text box. (You'll probably want to use the sharename that was previously assigned to this resource.)

   Note: If this shared resource is a disk device, move to the column of option buttons labeled *Permissions*. Mark the check boxes for the access permissions that you want.The *Admin only* check box is the **P** access permission.

8. Select the *OK* command button.

Example
You want to change the password and access permissions for the *\\print2\scratch* directory. Specifically, you want to add the **W** access permission and to remove the **X** and **A** access permissions.

You log on as the administrator and use the Full Screen Net Admin Interface to access the *\\print2.serve* server, using the instructions in the section of this appendix entitled, *Logging On As the Administrator*.



You select the *View* menu and select the *This server* menu item. In the *Resources This Server Is Sharing With the Network* dialog box, you select the *scratch* directory from the list box and select the *Delete* command button. When you select the *OK* command button in the confirmation dialog box, the *Resources This Server Is Sharing With the Network* dialog box reappears; you can see that the *scratch* directory is gone.

You select the *Add share* command button. The *What would you like to share?* dialog box appears. Then you select the *Disk directory* option button and select the *OK* command button. The *Share a Disk Resource With the Network* dialog box appears.

You type the same sharename, path, and remark for this resource as last time. In the *Password* text box, you type the new password. Moving to the *Permissions* option buttons, you select the *Read, Write, Create*, and *Delete* option buttons and select the *OK* command button. The *\\print2\scratch* directory is shared again, but with a different password and set of access permissions.

A2.8.2. Equivalent net Command

You may also change the password for a shared resource using the **net share** command. However, you must first delete the existing sharename and then recreate the sharename with the changed password. For more information about the **net share** command, see Chapter 10, *Command Directory*.

A2.9. Clearing or Changing the Administrative Password using the net Command

You can change the *ADMIN$* password using the *net password* command. For more information about the **net password** command, see Chapter 10, *Command Directory*.

A2.10. Assigning Remote UNIX System Process Execution Privileges

The Server Program allows users who are members to remotely execute UNIX system commands and programs on the server. Unlike using a terminal emulator to execute UNIX system commands, using the remote execution feature of **uexec** maintains the full functionality of a client. Users can execute a UNIX system command from their client's DOS or OS/2 command line, and immediately resume working with a shared directory or application. Remote UNIX system commands can run in the foreground or background and users can monitor and kill commands running in the background. Users execute remote UNIX system processes by invoking the **uexec** command.

When operating in share-level security mode, the LAN Manager server will accept **uexec** requests only if the following conditions are met:

* The user making the request is in a server directory that has uexec access permissions. To add **uexec** access permissions to a directory, see the procedure in this section.

* The user must specify an appropriate drive identifier for the **uexec** command's *driveid* parameter. This drive identifier must be linked to a directory on the server where the user has read, write, create, delete, and **uexec** access permissions.



You may wish to create a special directory for this purpose. If so, when creating the directory, you should indicate that it is for **uexec** use in the *Comment* text box. When users list available directories on the server, they will be able to read this comment.

To assign read, write, create, and delete access permissions to the directory, use the Full Screen Net Admin Interface, as described in the section of this appendix entitled, *Changing Access Permissions*. To add **uexec** access permissions to a directory, see the procedure in this section.

A2.10.1. Procedure

You assign **uexec** access permissions by using the *lmshare* program from the server console.

Use the following steps:

1. Log in as *root* at the server console-

2. Type

   ```
   cd /usr/net/servers/lanman
   ```

   and press RETURN.

3. Type

   ```
   lmshare -u sharename 1
   ```

   and press RETURN where *sharename* is replaced with the name of the shared resource to which **uexec** access permission is assigned.

4. Repeat step 3. If you wish to assign **uexec** access permissions to more shared server directories.

If you wish to remove **uexec** access permissions to a shared server directory, type

```
lmshare -u sharename 0
```

and press RETURN where *sharename* is replaced with the name of the shared resource from which **uexec** access permissions are to be removed.

B. Managing Logon Validation

B1. Overview

This appendix includes the following information:

* A description of logon validation
* The procedures required to set up logon validation
* Information about managing logon scripts

The logon validation can be used only by servers running user-level security.

B2. What Is Logon Validation?

Logon validation provides an additional measure of control over who can and can not access the LAN. If logon validation is used on the LAN, users are required to log on to the network before they can access any shared resources.

Note: If you choose not to use logon validation, server resources are still protected by the user-level or share-level resource security mode set up on the server.

To log on to the network, the user must supply a valid username and password. This user information is stored on the client and verified when the user tries to access a server resource. A server (running both user-level security and logon validation) immediately verifies the user's logon request, before the user can attempt to access a server resource.

A server that can validate logon requests is known as a *logon validator*. To validate logon requests, the server must have logon validation enabled after the Server Program is installed. In addition, servers that validate logon requests *must* be running user-level security (other servers on the LAN, however, may be running either user-level or share-level security). In addition, a logon validator's servername cannot be more than 13 characters long. Complete instructions for setting up logon validation appear in the section entitled *Setting Up Logon Validation*, p.B-4).

If you choose to enable logon validation, you will need to understand these concepts:

* Centralized logon validation
* Distributed logon validation
* Logon scripts (optional)

When you implement logon validation, you must specify which type of logon validation (centralized or distributed) that you wish to use.

B2.1. Centralized Logon Validation

Under centralized logon validation, you designate one server as the central logon validator. When a user logs on to the network, this server checks the username and password and either grants or denies access to the LAN. Centralized logon validation should be performed by a server that is always available when users need to access the LAN.

Centralized logon validation is best for small LANs or for LANs centered around a single server. Centralized logon validation has the following advantages:

* There is only one server maintaining a central account database. Other servers may have their own account databases, but the central server is a gateway through which all users must pass.

* By changing a user's account on the central server, you can affect that user's access to the entire LAN.

* For LANs made up of servers running share-level security, a central server (running user-level security and acting as a logon validator) can serve as the sole method of controlling access to resources by username.

* The response a user receives when logging on will always be the same.

Centralized logon validation also has the following disadvantages:

* The central server must maintain accounts for all valid users on the entire LAN (not just the accounts for users who will access one server).

* The central server bears the burden of processing all requests to log on.This can affect the general performance of the server.

* If the central server is not running, no one can log on.

B2.2. Distributed Logon Validation

Under distributed logon validation, you divide the responsibility for validating users among multiple servers. When a user tries to log on to the LAN, the logon request is broadcast to all servers in the LAN group. Any server running the proper software can evaluate the username and password, with the following results:

* If a server recognizes the username and password as valid, it responds to and validates the logon request.

* If a server does not recognize the username and password, it does not respond. If no server responds to the logon request, the user cannot log on.

Distributed logon validation is best for large LANs or for LANs that divide well into clusters of users and computers.Distributed logon validation has the following advantages:

* Each server maintains accounts only for valid users of that server. You don't need to maintain duplicate user accounts on a central server and on the server where a user normally works.

* No single server bears the burden of processing all logon requests.

* If one server is not running, users may still be able to log on, provided that they have an account on one of the other servers.

Distributed logon validation also has the following disadvantages:

* You must maintain multiple account databases, on more than one server.

* You may have to change a user's account on several servers in order to affect the user's access to the entire LAN.

* A user can get inconsistent responses when logging on, if servers with different accounts for that user are validating logon requests. For example, if a user has an account on two servers there is no way of ensuring which server will validate that user's logon request. If the user wants to use a logon script, the script would have to be on both servers.

To run distributed logon validation, these conditions must be met:

* More than one server must be acting as a logon validator.

* A LAN user must have an account on at least one of the servers acting as a logon validator.

B2.3. Logon Scripts

Under either logon validation method (centralized or distributed), a server must validate each logon request. You can arrange it so that when a server recognizes a valid username and password, it sends a set of commands to run on the requesting computer. This set of commands is known as a *logon script*.

Logon scripts are optional. You can avoid using logon scripts altogether, use them only for certain users, or use them for all users.

A logon script ordinarily contains some LAN Manager commands that set up basic connections in the LAN. For example, if most users need to access the *mis.serve**data* directory every time they log on, a logon script can establish this connection automatically every time someone logs on to the LAN. A logon script can also contain OS/2 or DOS commands that provide information or prepare the user's computer for LAN

Manager operations. For example, a logon script could print a message on the user's screen about what resources are available on the network.

There are two ways you can use logon scripts:

* You can create a general logon script that gives everyone on the LAN the same basic setup. This approach is best for LANs where most users have the same resource needs.

* You can create multiple logon scripts, each tailored to meet the needs of individual users. For example, you could create one logon script for novice users and another for advanced users, or you could create special logon scripts for individual users. This approach is best for networks whose users have a wide variety of resource needs.

You can use a DOS or OS/2 batch file, an executable file, or a LAN Manager profile as a logon script. (For more information, see the section of this appendix entitled *Managing Logon Scripts*.)

B3. Setting Up Logon Validation

This section describes how to prepare the LAN for logon validation. This section applies to both centralized and distributed logon validation.

The following list summarizes the tasks required to make logon validation work on your LAN:

1. Make sure that any server that will act as a logon validator has a servername that is no more than 13 characters long.

2. Specify whether the LAN will use centralized logon validation or distributed logon validation. To do this, set the *centralized=* parameter in the server's *lanman.ini* file.

3. Set up user-level security on each server that is to be a logon validator.

   If centralized logon validation is used, one (and only one) server must be a logon validator. If distributed logon validation is used, more than one server can be a logon validator.

4. Enable the netlogon service on each server that will be a logon validator. To do this, set the *netlogon=* parameter in the server's *lanman.ini* file.

5. Prepare all clients for logon validation. To do this, set the value of the *logonserver=* parameter in each client's *lanman.ini* file to the appropriate value.

The following sections describe each of these tasks in detail.

B3.1. Changing a Logon Validator's Servername

You can change a logon validator's servername in either of the following ways:

* via the *listenname=* parameter of the server's *lanman.ini* file.

* If no value is given in the *listenname* parameter of the server's *lanman.ini* file, the server will be known as *uname.serve*, where *uname* is the UNIX system node name of the server computer. The UNIX system node name can be set and changed via *sysadm*. For more information on setting the UNIX system node name via *sysadm*, see *System Administration Guide, System V.*

If you cange the servername of your logon validator, make sure that all users whose clients use the server for logon validation specify their new name in the *logonserver=* parameter of the clients *lanman.ini* file. For more information, see *Supermax LAN Manager/X - Client Installation Guide.*

Note: Changing the machine name may disrupt network communications or the operation of other applications that depend on the use of the machine name.

The maximum length for a server's name is 14 characters. However, when you are setting up your network to use logon validation, the maximum length of a logon validator's servername is 13 characters (including the *.serve* extension).

If the length of the logon validator's servername exceeds 13 characters, users may receive the following error message when they try to start the Enhanced DOS Client Program:

```
NET2124:    Insufficient memory
```

B3.2. Setting Up Centralized or Distributed Logon Validation

You must first decide whether to run centralized logon validation or distributed logon validation.

Set the *centralized=* parameter in the *lanman.ini* file to the same value on every server on the LAN, even those that will not be logon validators, to reflect your choice of either centralized or distributed logon validation. You may decide later to run a different (or additional) server as a logon validator, and you need to be sure that all servers agree on the method of logon validation.

To specify whether the LAN should run centralized logon validation or distributed logon validation,perform the steps described in Chapter 9, *Changing Parameter Values with a Text Editor.*

B3.2.1. Setting Up User-Level Security

Logon validation involves checking usernames and corresponding passwords. Only servers running user-level security use this information. Servers running share-level security do not recognize usernames and their corresponding passwords. Therefore, any server that validates logon requests must be running user-level security. (For instructions concerning how to set up user-level security, see Chapter 4, *Setting Up A Server With User-Level Security*.)

Each user who will access the LAN must have a user account on at least one of the servers performing logon validation. When you set up the user account, you must mark the Use script check box in the *Add User Account* dialog box. (For instructions concerning how to set up user accounts, see Chapter 6, *Managing Users and Groups Under User-Level Security*.

B3.2.2. Starting the Netlogon Service

Logon validation is a LAN Manager service. Each server that is to validate logon requests must be running the netlogon service:

* If the LAN is running centralized logon validation, only one server should be running the netlogon service. This server will be the only server on the LAN to validate logon requests.

* If the LAN is running distributed logon validation, many servers can be running the netlogon service. These servers will all be capable of validating logon requests.

Clients and other servers do not need to run this service.

To start the netlogon service, set the *netlogon=* parameter in the *lanman.ini* file to *yes*. Do this by performing the steps described in Chapter 9, *Changing Parameter Values with a Text Editor* at each server on the LAN that will validate logon requests.

B3.2.3. Preparing Clients

You have now prepared the LAN's servers for logon validation. The LAN's clients also must be prepared to work under logon validation. This is done by entering a value for the *logonserver=* parameter in the client's *lanman.ini* file. The type of entry you use for this parameter may vary, depending upon the type of logon validation (centralized or distributed) that is being used on the network.

Your purpose in preparing the client is to ensure that it will send logon requests to the logon validator server(s).

If it is impractical for you to set up all of the individual clients on the network yourself, you can send instructions to the users of the clients so that they can make the necessary change themselves.

To prepare clients for logon validation, make the appropriate change to the *lanman.ini* file on each client on the network:

* If the network is running centralized logon validation, change the *logonserver=*-parameter in the client's *lanman.ini* file so that it reads

  logonserver=\\server.serve

  where *server* is the name of the central server performing logon validation on the network.

  Every client on the network should have this line in its *lanman.ini* file.

* If the network is running distributed logon validation, change the *logonserver=* parameter in the client's *lanman.ini* file as appropriate:

  - If you want a specific server to validate logon requests that originate from this client, change the parameter so that it reads

    logonserver=\\server.serve

    where *server* is the name of the specific server that you want to validate logon requests that originate from this client. If the user of this client does not have an account on that server, the user will not be able to log on to the network.

  * If you want the client to broadcast logon requests to all available servers, change the parameter so that it reads

    logonserver=*

    Any logon validator server with an enabled account for the requesting user can respond.

Make sure that you have entered the appropriate value for the *logonserver=* parameter on every client on the network (the value you enter can vary from one client to another).

Example
You have set up *humanr.serve* as the central logon validator for your network. Due to the size of the network, it would be very difficult for you to prepare all of the clients yourself.

You send out a memo to all users of the network, telling them to edit the *logonserver=* parameter of their client's *lanman.ini* files to read

logonserver=\\humanr.serve

You have now prepared all of the clients on the network to use logon validation. If you want, you can now create logon scripts for users (see the section of this chapter entitled *Managing Logon Scripts*, for instructions on how to make and use logon scripts).

B4. Maintaining Logon Validation

To maintain logon validation, perform the following tasks regularly:

* Maintain the user accounts on servers functioning as logon validators. Under centralized logon validation, the central server must have an account for every possible user, and each account must have logon validation enabled. Under distributed logon validation, each possible LAN user must have an account on at least one of the logon servers, and for each user, at least one account must have logon validation enabled.

* Maintain consistency across the LAN. All servers must agree on the method of logon security (centralized or distributed). Make sure that each new server conforms with the others on the network.

* Maintain logon scripts. If the LAN uses logon scripts, make sure that they accurately reflect the needs of the LAN and its users.

B5. Managing Logon Scripts

Logon scripts are files that contain OS/2, DOS, or LAN Manager commands. If a server is a logon validator, you can set it up to run logon scripts for users each time they log on to the network. The following sections provide detailed instructions for using and creating logon scripts.

B5.1. Using Logon Scripts

To use logon validation, you must enable logon validation for each user account on at least one server that will act as a logon validator.

Important: When you start the netlogon service, it automatically shares the *userdirs* directory with the sharename *users*. Do not delete this sharename; it gives users access to their home directories.

If you want a user to be able to use a logon script, you must ensure that the following two conditions are met when you create the user account:

1. The *Use script* check box must be marked in the *Change User Account* dialog box. This enables the server to validate the user when he or she attempts to log on to the network.

2. The name (or pathname) for the file containing the logon script must appear in the *Script* text box. The logon script in this file will be run every time the user logs on to the network.

   Note: If you don't want a logon script to run when the user logs on, leave the *Script* text box blank.

The Server Program provides two default logon scripts, *scripts netlogon.bat* (for Enhanced DOS clients), and *scripts netlogon.cmd* (for OS/2 clients). In response to a logon request, these logon scripts

* display the name of the server that is validating the logon request. If you don't supply this information with a logon script, the user cannot be certain which server has responded to the logon request.

* establish a connection to the user's home directory (if there is one) on the server.

Keep logon scripts in the server's */usr/lanman/scripts* directory (if there is a */usr2* file system, use the default directory, */usr2/lanman/scripts*). The Full Screen Net Admin Interface expects all pathnames for logon scripts to be relative to the */usr/lanman* directory, either in the scripts subdirectory or in the individual home directories of users. You can change the location or name of the */usr/lanman* directory by changing the value of the *userpath=* parameter in the *lanman.ini* file.

Example
You have set up a user account for John O'Clare (*johnoc*) on the *humanr.serve* server. You now want to enable logon validation for the *johnoc* account.

You use the Full Screen Net Admin Interface to access the *humanr.serve* server and select the *Accounts* menu. You then select the *Users/groups* menu item. In the *Users/Groups* dialog box, you move to the *Username* list box and select *johnoc*. You then select the *Zoom* command button.

In the *Change User Account* dialog box, you note that the *Use script* check box is marked, showing that this server will validate *johnoc*'s logon requests. You move to the *Script* text box and type `scripts\netlogon.cmd`, the name of the default logon script (John is using an OS/2 client; if he had an Enhanced DOS client, you would need to specify the name of the *scripts\netlogon.bat* file).

B5.2. Creating Logon Scripts

You can create your own logon scripts if you choose not to use the default logon script. You can create any of three kinds of logon scripts: DOS Batch files or OS/2 CMD files; Programs (executable files); LAN Manager profiles.

Place all logon scripts in the */usr/lanman/scripts* (or the */usr2/lanman/scripts*) directory.

B5.2.1. DOS Batch Files or OS/2 CMD Files

When you create a batch file or CMD file as a logon script, you can put any OS/2, DOS, or **net** commands in it, with the following restrictions:

* Do not use the **net logoff** command inside a logon script. There is no way to stop a logon request from inside a logon script.

* Errors that occur during the running of the logon script do not stop the logon procedure. The user receives an error message and the logon continues.

DOS batch files are for Basic DOS and Enhanced DOS clients only; OS/2 CMD files are for OS/2 clients only. Assign the type of file that corresponds to the operating system that the user will be using.

Table B-1 summarizes the variables available in a batch or CMD file logon script.

Table B-1. Batch or CMD File Script Variables

Variable	Meaning
%1	The username of the user requesting logon validation
%2	The computername of the logon validator server
%3	The sharename of the */usr/lanman* directory (or the */usr2/lanman* directory, if it exists)
%4	The path of the user's home directory, relative to */usr/lanman* (or */usr2/lanman*, if it exists)

Examine the server's */usr/lanman/netlogon.cmd* (or */usr2/lanman/netlogon.cmd*, if it exists) logon script file for an example of how these variables can be used.

For more information about batch file or CMD file programming, see your DOS or OS/2 manual.

B5.2.2. Programs (Executable Files)

You can create a DOS or OS/2 executable file (program) as a logon script. Use whatever means you like to create the program. The four variables available to batch and CMD files (see Table B-1) are also passed to programs.

B5.2.3. LAN Manager Profiles

This is the simplest way to create logon scripts. To do this, you set up a client (establishing all of the appropriate links that you want the profile to establish), save a copy of that setup, and use the copy as a profile script.

To create a profile script, follow these steps:

Note: Create the profile script from a client. Ideally, use the client on which this profile script will run.

1. Using the Full Screen Net Interface, or with **net** commands, establish the links (to network resources) that you want to save in the profile script. If you specify redirected drive letters, use letters that will not conflict with client devices. For example, some clients may have a hard drive D, so you may not want to use any letter before E as a devicename in a profile.

2. Start the Full Screen Net Interface by typing `net` at the client's system prompt. Press RETURN.

3. Select the *Config* menu and select the *Save* profile menu item.

   The *Save Configuration* dialog box appears.

4. Type the name of the profile you wish to save in the *Filename* text box.

5. Select the *OK* command button.

   A confirmation message appears, showing the location of the new profile on the client's hard disk.

6. Select the *OK* command button.

   The system returns you to the background screen.

7. Move the profile to the */usr/lanman/scripts* directory on the server (or the */usr2/lanman/scripts*, directory, if it exists).

8. Start the Full Screen Net Admin Interface and access the server you wish to administer (this must be the same server containing both the profile and the user accounts that you want to use the profile).

9. Select the *Accounts* menu and select the *Users/groups* menu item.

   The Users/Groups dialog box appears.

10. Highlight the name of a user you wish to use the profile in the *Username* list box.

11. Select the *Zoom* command button.

    The *Change User Account* dialog box appears.

12. Make sure that the *Use script* check box is marked.

13. Enter the path for the profile you just created in the *Script* text box. The proper format is

    SCRIPTS\profile.pro



where *profile.pro* is the name of the script you just created.

14. Select the *OK* command button.

    * If the user has a home directory on the server, the *Edit File Permission* dialog box appears. You do not need to change the information in this dialog box. Select the *OK* command button. The *Users/Groups* dialog box appears.

    * If the user does not have a home directory on the server, the *Users/Groups* dialog box appears.

15. Proceed as appropriate:

    * If you want to change the user accounts for additional users, return to Step 10.

    * If you do not want to change the user accounts for additional users, proceed to Step 16.

16. Select the *Done* command button.

    The system returns you to the background screen.

Example
You want to create a logon script for new users that performs these functions:

* Links to the *humanr.serve**public* directory as the local *P* drive.

* Links to the *print1.serve**laser* spooled printer queue as the local *LPT1:* device.

From an Enhanced DOS or OS/2 client, you use the Full Screen Net Interface or the **net use** command to make the desired links. From the *Config* menu, you select the *Save profile* menu item. In the *Save Configuration* dialog box, you type the filename *newusers.pro* in the *Filename* text box and select the *OK* command button to create the profile. The profile is saved in the client's *PROFILES* directory.

Since you are an administrator on the *humanr.serve* server, you can use the special *C$* resource, representing the server's C: drive. At the system prompt, you link to the server's hard disk by typing **net use f: \\humanr.serve\C$** and pressing RETURN. You make the f: drive the active drive by typing **f:** and pressing RETURN. Then you move to the *scripts* directory by typing **cd usr2\lanman\scripts** and pressing RETURN (if your server did not have a */usr2* directory, you would have to type **cd usr/lanman/scripts**).

Now you copy the newly created profile from the client's *PROFILES* directory to the server's *scripts* directory.

Once the file has been copied, you can specify *newusers.pro* in the *Script* text box when adding new users to the server.

B5.2.4. Equivalent net Command

You may also save a LAN Manager profile script by using the **net save** command. Specify the file name of the script file with the **net user** command, with the */script* option. For more information about the **net save** and **net user** commands, see Chapter 10, *Command Directory*.

INDEX

Access permissions
    accessing resources 4-13
    changing by non-administrators 7-14
    changing for disk resources 7-11
    changing security A-12
    checking 7-10, A-9
    default 7-14
    description 4-3
    disk resource 4-4, 7-8, 7-11
    explicit 7-14
    hierarchy 4-4
    inherited 7-14
    print resources 8-11
    share-level security A-1
    shared directories 4-31
    shared print queues 4-6, 4-37, 8-10, 8-11
    user-level security 4-4
Access to resources under share-level security A-2
accessalert= parameter 9-4
accessfile= parameter 9-8
accessgroup= parameter 9-8
accesshi= parameter 9-8
accesslow= parameter 9-8
accessmed= parameter 9-8
accessowner= parameter 9-8
accessperms= parameter 9-8
Accounts menu
    see Full Screen Net Admin Interface
Adding groups to the server 10-37
Adding user accounts 4-22
Adding user groups 4-20
admin password 5-7
admin privilege level 4-3
admin user account 4-2
ADMIN$ resource A-2, A-4
admingroupid= parameter 9-9
Administering shared printer queues 10-44
Administering Supermax LAN Manager/X
    from client 10-1
    from server 10-3
    via the Command Line Net Interface 10-1
Administering the server from client 4-15, A-6
Administrator responsibilities 2-5
adminpath= parameter 9-9
adminuserid= parameter 9-9
Alerter service 4-18
alertnames= parameter 9-4

alertthresh= parameter 9-9
anncmailslot= parameter 9-9
ASCII text files 2-3
Audit Trail 2-2, 10-19
    auditing= parameter 2-2, 9-4
    description 2-2
    displaying 5-2
    setting up 4-19
auditing= parameter 9-4
audlogfilename= parameter 9-9
audloggroup= parameter 9-9
audlogowner= parameter 9-10
audlogperms= parameter 9-10
autodisconnect= parameter 9-4

Background screen 3-4
    see Full Screen Net Admin Interface
Backing up server files 7-20
Batch files as logon scripts B-9
byemessage= parameter 9-10

Centralized logon validation 2-5, B-2
centralized= parameter 2-5, 9-28
Changing access permissions for disk resources 7-11
Changing an administrative password 5-7
Changing shared print queues options 8-16
Changing shared print queue status 8-19
checkpoint= parameter 9-10
Client printers 8-1
    see Shared client printers
Client Program
    and server administration 4-15, A-6
    installing 1-2
    logon validation B-6
    starting 4-15, A-6
Closing shared files 10-35
clstructs= parameter 9-10
CMD files as logon scripts B-9
Command button
    Zoom 3-16
Command buttons 3-15
    Cancel 3-16
    OK 3-16
Command Line Net Interface 3-1
    from client 10-1
    from server 10-3
Command-Line administration utility 5-8
Commands
    abbreviations 10-5

net access 10-12
net admin 10-17
net audit 10-19
net config server 10-22
net continue print 10-27
net device 10-29
net errors 10-32
net file 10-35
net group 10-37
net load 10-40
net pause print 10-42
net print 10-44
net save 10-52
net send 10-54
net separator 10-56
net session 10-58
net share 10-61
net statistics 10-69
net status 10-71
net user 10-72
passwords 10-5
syntax 10-7
Configuring
printers 4-32
share-level security A-5
server 9-1, 10-22
Connect to a Remote Server
dialog box 3-3
Continuing paused services 10-27
Controlling
access to shared resources 10-12
print jobs 8-23
sessions 10-58
shared printers 10-29
shared resources 10-40
user accounts 10-72
controllock= parameter 9-10
Conventions 1-2, 10-8
Copying sharelists 10-52
copyright= parameter 9-10
cpipgroup= parameter 9-10
cpipname= parameter 9-11
cpipowner= parameter 9-11
cpipperms= parameter 9-11
createhomedir= parameter 9-11
Customized print processor scripts 8-13

Daily network\server tasks 2-6

DDE-Term
    Terminal Emulation 2-3
debug= parameter 9-11
debugdir= parameter 9-11
debugpat= parameter 9-11
debugsignal= parameter 9-11
debugsize= parameter 9-12
Default access permissions 7-14
Design and installation of the network 2-6
Dialog boxes 3-7
    Full Screen Net Admin Interface 3-16
    moving around in 3-8
    using check boxes 3-14
    using command buttons 3-15
    using display fields 3-16
    using list boxes 3-10
    using option boxes 3-15
    using text boxes 3-9
dirbufsize= parameter 9-12
Directories
    see Shared directories
dirperms= parameter 9-12
Disk organization 4-11
Disk resource access permissions 4-4, 7-8, 7-11
Disk space 7-19
Display fields 3-16
Distributed logon validation 2-5, B-2
DOS batch files as logon scripts B-9
DOS-to-UNIX System format traslation 2-3
Duties of administrators 2-5

Educating users 2-7
Enhanced DOS client 4-15, A-6
errlogfilename= parameter 9-12
errloggroup= parameter 9-12
errlogowner= parameter 9-12
errlogperms= parameter 9-12
erroralert= parameter 9-4
errorhi= parameter 9-12
errorlow= parameter 9-12
errormed= parameter 9-13
exclude= parameter 9-28
Executable files as logon scripts B-10
Exiting
    Full Screen Net Admin Interface 3-16
Explicit access permissions 7-14

File locks 10-35
fileperms= parameter 9-12

Files
    backup 7-20
    restoring 7-20
    translation 2-3
forceunique= parameter 9-29
Full Screen Net Admin Interface
    accessing server 3-2
    background screen 3-4
    defining print processor scripts 8-15
    description 3-1
    exiting 3-16
    listing shared directories 7-1
    Message menu 5-1
    sharing print queues 8-5
    starting 10-17
    status menu 5-2
    using 3-2
    View menu 4-28, 7-3, A-7
    working with 3-3
Full Screen Net Interface
    help 3-3

gcbuffer= parameter 9-13
getapipe= parameter 9-13
Groupnames 4-9
guest privilege level 4-3
Guest user account 4-2

Hardware
    installation 1-2
hashsize= parameter 9-13
Help 3-3
hiprimailslot= parameter 9-13
Home directories 4-24

ignoreunix= parameter 9-13
Implementing server configuration
    illustration 4-17
Inherited access permissions 7-14
Installation prerequisites 1-2
Interfaces 3-1
ipctries= parameter 9-13

keepadmshares= parameter 9-14

LAN group 5-4
LAN Manager Resource Permissions 4-4
langroup= parameter 9-29

lanman.ini file
changing parameters using a text editor 9-32
changing parameters with srvconfig. program 9-32
description 9-1
lmxserver section 9-8
location 9-1
netlogon section 9-28
organization 9-3
sample file 9-31
server section 9-4
syntax 9-2
uidrules section 9-28
ups section 9-29
workstation section 9-28
List boxes 3-10
listenextension= parameter 9-14
listenname= parameter 9-4
Listing print jobs 8-23
Listing shared directories 7-1
lmxmsgfile= parameter 9-14
lmxserver section of the lanman.ini file 9-8
lmxsrv= parameter 9-14
Locks 10-35
Logging on as the administrator 4-15, A-6
Logon B-5
as administrator 3-2
Logon scripts
creating B-9
defaults 4-24
description 2-5, B-3
DOS batch files B-9
OS\2 CMD files B-9
profile scripts B-10
program files B-10
user accounts 4-24
using B-8
Logon validation
centralized 2-5, B-2
centralized= parameter 9-28
creating logon scripts B-9
description 2-4, B-1
distributed 2-5, B-2
logon scripts B-3, B-8
maintaining B-8
netlogon service B-6
netlogon= parameter 9-17
preparing clients B-6
setting up 4-16, B-5
logonalert= parameter 9-5

logonhi= parameter 9-14
logonlow= parameter 9-14
logonmed= parameter 9-14
lp subsystem
    and shared print queues 8-1
    and the print processor option 8-4
lptmpdir= parameter 9-14

mailslotgroup= 9-14
mailslotowner= parameter 9-15
mailslotperms= parameter 9-15
maxadminoutput= parameter 9-15
maxauditlog= parameter 9-5
maxclients= parameter 9-5
maxerrlog= parameter 9-5
maxfilesize= parameter 9-15
maxlocknap= parameter 9-15
maxmsdepth= parameter 9-15
maxmsgsize= parameter 9-15
maxmux= parameter 9-15
maxreadsize= parameter 9-15
maxvcperproc= parameter 9-16
maxwritesize= parameter 9-16
Menus
    using 3-5
Message menu
    Full Screen Net Admin Interface 5-1
Message service
    see Network Message service
minpassword= parameter 9-16
minvcperproc= parameter 9-16
msdirgroup= parameter 9-16
msdirname= parameter 9-16
msdirowner= parameter 9-16
msdirperms= parameter 9-17
msgheader= parameter 9-17

Names
    groupnames 4-9
    sharenames 4-10
    usernames 4-9
net access command 7-14, 7-17, 10-12
net admin command 10-17
    options 3-2
net audit command 10-19
    net 10-19
net commands
    abbreviations 10-5
    administrators only 10-9

and passwords 10-5
syntax 10-7
using 10-1
net config server command 10-22
net continue command 8-23
net continue print command 10-27
net device command 8-26, 10-29
net error command 10-32
net file command 10-35
net group command 4-22, 10-37
net load command 10-40
net logoff command B-9
net password command 5-8, A-16
net pause command 8-23
net pause print command 10-42
net print command 8-19, 8-21, 8-26, 10-44
net save command 10-52, B-13
net send command 10-54
net separator command 10-56
net session command 10-58
net share command 4-38, 5-7, 7-18, 8-11, 8-16, 10-61, A-9, A-16
changing access permissions A-12
changing passwords A-13
net statistics command 10-69
net status command 10-71
net user command 4-28, 4-32, 7-8, 10-72
nethelpfile= parameter 9-17
netlogon section of the lanman.ini file 9-28
netlogon service B-6
netlogon.bat file 4-24
netlogon.cmd file B-9
netlogon= parameter 9-17
netmsgfile= parameter 9-17
netosmsgfile= parameter 9-17
Network Message Service 2-2
Network troubleshooting 2-7
network= parameter 9-17
newusershell= parameter 9-18
nfslocks= parameter 9-18
nonexistusers= parameter 9-18
nosendtime= parameter 9-19

Option buttons 3-15
Options for shared print queues 8-2
Organizing server disks 4-11
OS/2 client 4-15, A-6
OS/2 CMD files as logon scripts B-9

Parameters
changing with a text editor 9-32
changing with srvconfig program 9-32
description 9-1
relative pathnames 9-2
syntax 9-2
Parameters option 8-5
passmgmt= parameter 9-19
Passwords
admin 5-7, A-16
administrative passwords 5-7, A-16
changing security A-13
checking security A-9
share-level security A-1
user-level security 4-2
Pausing shared printers 10-42
Permissions
see Access permissions
poweraddr= parameter 9-29
powermessage= parameter 9-29
powertime= parameter 9-29
Prerequisites
Supermax LAN Manager/X 1-2
Print processor option 8-4
Print processor scripts
defining 8-15
description 8-2
environmental variables 8-14
guidelines 8-13
samples 8-14
using 8-13
Print queues
see Shared print queues
sharing 8-5
unsharing 8-15
Print services
Print 2-1
Printer devicename option 8-3
Printers
access permissions 8-11
configuring 4-32
managing 8-16
see Shared client printers
see Shared print queues
Privilege levels 4-3
prodname= parameter 9-19
Profile scripts used as logon scripts B-10
Program files as logon scripts B-10

qsched= parameter 9-19
Queue priority option 8-4
queuealloc= parameter 9-19

rdatrend= parameter 9-19
Relative pathnames directory 9-2
relmajor= parameter 9-20
relminor= parameter 9-20
Remote administration 2-1
Remote UNIX system processes 2-3, A-16
Removing file locks 10-35
Resource auditing 4-19
Resource IPC$ A-4
Resource security
    see Share-level security
    see User-level security
Resource share-level security
    IPC$ A-4
Restoring server files 7-20

sbstelladmin= parameter 9-20
sbstelluser= parameter 9-20
Scheduling option 8-4
Scripts
    see Logon scripts
    see Print processor scripts
Security for servers
    see Share-level security 2-4
    see User-level security 2-4
security= parameter 9-6
Sending files 10-54
Sending messages 10-54
Separator page option 8-5
Server
    administering via net commands 10-5
    backing up files 7-20
    disk organization 4-11
    disk space 7-19
    displaying information 10-22
    listing shared resources 5-4
    listing visible servers 5-4
    restoring files 7-20
    security 2-4, A-5
    status 10-69
    troubleshooting 2-7
Server program
    configuration. See lanman.ini file 9-1
    features 2-1
    services 2-1

stopping 5-1
server section of the lanman.ini file 9-4
Sessions
disconnecting 10-58
listing 10-58
Share-level security
access permissions A-1, A-9, A-12
accessing resources A-2
ADMIN$ resource A-4
administration A-2
changing access permissions A-12
changing passwords A-13
configuring A-5
decription 2-4
passwords A-1, A-9, A-13
planning server setup A-5
remote UNIX system processes A-16
setting up a server A-4, A-5
shared directories A-6
special administrative resources A-3
Shared client printers 8-1
Client printers 2-1
Shared directories 4-28
assigning access permissions 4-31, 7-6
creating 4-28, 7-2, A-6
default 4-10
linking to defsult directories path statement 4-11
listing 7-1
locations 4-11
organizing 4-11
planning 4-10
sharename 4-29, A-8
specifying a sharename 7-4
unsharing 7-17
Shared files 10-35
Shared print queues
access permisions 4-6, 4-37
access permissions 4-6, 8-10, 8-11
changing options 8-16
changing status 8-19
configuration 4-33
creating, using Full Screen Net Admin Interface 8-5
description 4-6
listing print jobs 8-23
managing 8-16
operation 8-2
options 8-2
parameters 8-5
planning 4-10

print processor option 8-4
printer devicename option 8-3
queue priority option 8-4
scheduling option 8-4
separator page option 8-5
sharename 4-33
specifying sharename 8-7
unsharing, using the Full Screen Net Admin Interface 8-15
Shared printer queues 10-44
Shared printers 10-29
see Shared print queues
Shared resources
sharing 10-12, 10-61
sharefile= parameter 9-20
sharegroup= parameter 9-20
Sharelists
loading 10-40
saving 10-52
Sharenames
creating 4-10
shared directories 4-29, A-8
shared print queues 4-33
specifying for shared directories 7-4
specifying for shared print queues 8-7
shareowner= parameter 9-20
shareperms= parameter 9-20
Sharing directories 7-2, A-6
Sharing print queues 4-33
Sharing special administrative resources A-3
shmgroup= parameter 9-20
shmowner= parameter 9-21
shmperms= parameter 9-21
spareserver= parameter 9-21
spipe= parameter 9-21
srvannounce= parameter 9-6
srvcomment= parameter 9-6
srvheuristics= parameter 9-6
srvhidden= parameter 9-6
srvstathelpfile= parameter 9-21
srvstatmsgfile= parameter 9-21
stacksize= parameter 9-21
Starting
Client Program 4-15
Full Screen Net Admin Interface 10-17
netlogon service B-6
printers 10-27
Starting the LAN Manager Client Program A-6
startscript= parameter 9-21

Statistics
server 10-69
Status menu 5-2
stoponcore= parameter 9-22
Stopping the server program 5-1
Supermax LAN Manager/X
prerequisites 1-2
svcinit= parameter 9-22
svcscript= parameter 9-22
Syntax of the lanman.ini file 9-2

Text boxes 3-9
Text File Translation 2-3
threshold= parameter 9-22
Translating DOS-to-UNIX system file format 2-3
Troubleshooting 2-7

uexec command 2-3, 4-3, A-16
uexec user group
description 4-2
uexecaccadd= parameter 9-22
uidrules section of the lanman.ini file 9-28
UNC names 4-11
Universal Naming Convention names
UNC names, description 4-11
UNIX system processes
See Remote UNIX system processes
unixlocks= parameter 9-22
Unsharing directories 7-17
ups section of the lanman.ini file 9-29
User accounts 10-72
accessing resources 4-13
adding 4-22
admin 4-2
creating 4-22
description 4-2
guest 4-2
home directories 4-24
planning 4-8
privileges 4-3
User education 2-7
User groups
accessing resources 4-13
adding 4-20
creating 4-20
default 4-2
description 4-2
planning 4-8

shared directories 4-11
uexec 4-2
users 4-2
User interfaces 3-1
User-level security
access permissions 4-3, 4-6, 7-10, 7-11
accessing resource illustration 4-7
description 2-4, 4-1
disk resource access permissions 4-4
logon validation 4-16, B-6
passwords 4-2
printer configuration 4-32, A-9
privilege levels 4-3
resource organization 4-9
server configuration 4-8
server set up 4-8
shared directories 4-28
shared print queue access permissions 4-6
user accounts 4-2
user groups 4-2, 4-20
usernames 4-2
Usernames
creating 4-9
description 4-2
userpath= parameter 4-24, 9-6
userremark= parameter 9-23
users user group 4-2
Using text boxes 3-9
Using UNC names 4-11
ustructs= parameter 9-23
util directory
description 4-11
util2 directory
description 4-11
uxclosecount= parameter 9-23

vcdistribution= parameter 9-23
Visible servers 5-4

workstation section of the lanman.ini file 9-28

Zoom command button 3-16