Administering
Advanced Server For UNIX Systems

December, 1995
Version 1.2

Stock No. 94424201

Advanced Server For UNIX Systems Addendum for Administering LAN Manager for UNIX Systems

December, 1995
Version 1.2

Stock No. 94424201

Introduction

This addendum contains information about the changes that have been made to the *Advanced Server for UNIX version 2.2* since the *Administering LAN Manager for UNIX Systems* manual was written.

This addendum describes changes only.

Further Information

DDE has the following manuals, containing further information about Advanced Server 2.2 for UNIX:

DDE *Stock Number*	*Title*
94424201	Administering Advanced Server 2.2 for UNIX Systems
94424211	Advanced Server 2.2 for UNIX Systems Troubleshooting and Command Reference
94424221	Advanced Server 2.2 for UNIX Systems Installation and Configuration Guide
94424231	LAN Manager User's Guide for MS-DOS
94424241	LAN Manager User's Guide for MS OS/2
94424251	Using LAN Manager with MS Windows
94424261	NetWare Connectivity Administrator's Guide
94424281	Advanced Server 2.2 for UNIX Systems Hints

General and repeated inconsistencies

The UNIX **`sysadm`** program is generally referred to as **`sysadmin`**.

The ASU product is referred to as LAN Manager, also in the titles of additional documentation.

Overview, p. v

Administering Advanced Server 2.2 for UNIX Systems is intended for the administrator who will configure the Advanced Server 2.2 for UNIX Systems installed on a Supermax Enterprise

Server running UNIX System V Release 4.2MP version 1.2 and higher or Supermax Multiserver System V Release 3.1 Version 8.0 and higher.

Related Documentation, pp. x-xi

See the list earlier in this addendum. The list on pp. x-xi contains Remoteboot Guide, NetBEUI Transport Guide and Multiprocessor Activator, which are not available, as remoteboot is not implemented, NetBIOS over TCP/IP used instead of NetBEUI, and a Multiprocessor Activator is neither necessary on a Supermax Enterprise Server nor on Supermax Multiserver.

Guarding Against Data Loss, p 1-12

UPS is not supported on the Supermax Enterprise Server or the Supermax Multiserver version of the product.

Remote Administration, p. 1-13

Besides from the LAN Manager 2.2 client or the MS OS/2 client, the server can also be remotely administered from a Windows 3.1/3.11 client running the netadmin program.

Remote Booting, p. 1-13

Remote booting of clients is not supported in Advanced Server 2.2 for UNIX Systems.

Netrun Service, p. 1-13

The `netrun` service is both on the MS OS/2 Clients and the DOS Clients, but not on the Windows for Workgroups 3.11 clients.

Logging In to the UNIX System with the Kermit Terminal Emulator p 2-32

The Kermit Terminal Emulator software is not supported on the Supermax Enterprise Server or the Supermax Multiserver.

Planning Resource Access Permissions, p. 3-27

The permission abbreviation ACDR does not correspond to "create, delete, read write and execute"; instead it corresponds to "attribute change, create, delete and read".

Sharing Remote Directories Using NFS and RFS, pp 5-11 to 5-16

All information about RFS should be ignored, as this is not supported on the Supermax Enterprise Server or the Supermax Multiserver.

This section contains specific information for NCR System 3000 NFS. This should be ignored.

Setting Permissions and Auditing for a Disk Resource, pp 5-18 to 5-19

There is an error in the typography ind Item 3, where only the string "setting permissions for" should be in the typewriter-like font.

Managing Shared Printers, pp 6-1 to 6-72

Besides the information in this chapter, please refer to "Advanced Server 2.2 for UNIX Systems Hints", the chapter on Printers.

Accessing the UNIX System Administartive Interface, pp 2-26

For Supermax Supermax Multiserver version of the product the LAN_Manager is changed to LANManager in the Note on page 2-26

Managing Server Operations, Chapter 7

The UPS service and the NValert services are not supported on ASU2.2 for Supermax Enterprise Server or the Supermax Multiserver.

p.7-23 : Pressing Ctrl+Alt+Del is the PC way of warm-booting the server. Corresponds to doing an init 6 or correspondingly on a UNIX server.

p. 7-64 : Specifying the Max Number of Sessions: Other intervals for the user upgrade packages apply to the Supermax Enterprise Server or the Supermax Multiserver Version of ASU2.2. See "Advanced Server 2.2 for UNIX Systems Hints", the section on upgrading the max. no. of users.

Appendix B: The Server's lanman.ini-file

The **`maxclient`** parameter's maximum value depends upon the installed user upgrade packages. Other intervals for the user upgrade packages apply to the Supermax Enterprise Server or the Supermax Multiserver Version of ASU2.2. See "Advanced Server 2.2 for UNIX Systems Hints", the section on upgrading the max. no. of users.

The **`srvcomment`** parameter is changed from "LAN Manager for UNIX Server" to "Advanced Server 2.2 for UNIX Systems".

The **`stacksize`** parameter's default value is changed from 10000 to 30000 bytes.

A parameter, **`useoplock`** is added. Its value is **`yes`** or **`no`**, default is **`yes`**. It determines whether oplocks should be used or not, that is, whether clients should have exclusive access to files whenever possible, until other clients requests access to the same file. Using oplocks improves performance in most cases.

A parameter, **`oplocktimeout`** is added. It's default value is 30 sec. and it can vary from 0 to 30 sec. It is the time that the server waits to break an oplock when requested, and the client does not respond.

The default value for **`deltabufsize`** is increased from 8KB to 16KB.

The default value for **`fsmap`** has been changed to **`vfxs:ufs, unknown:ufs, nfs:ufs`**. **`fsnosupport`** has been changed to **`ufs`** for Enterprise Server. For Supermax Multiserver the default value for **`fsmap`** is **`unknown:s5, nfs:ufs`**. **`fsnosupport`** has been changed to **`s5`**.

The **`runpath`** in netrun section of lanman.ini file can have multiple path entries delimited by colon (:) and not semicolon.

LAN Manager for UNIX® Systems

Administering LAN Manager

VERSION 2.2

An Advanced Network Server

NOTICE

The information in this document is subject to change without notice. NCR and Microsoft assume no responsibility for any errors that may appear in this document.

The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of the agreement. It is against the law to copy the software on any medium except as specifically allowed in the license or nondisclosure agreement.

TRADEMARK NOTICE

AT&T and StarGROUP are registered trademarks of American Telephone and Telegraph Company.
NetView, OS/2 and IBM are registered trademarks of International Business Machines Corporation.
Microsoft, MS, and MS-DOS are registered trademarks, and Windows is a trademark of Microsoft Corporation.
OS/2 is a registered trademark licensed to Microsoft Corporation.
NCR is a registered trademark of NCR Corporation.
UNIX is a registered trademark of UNIX System Laboratories.

Contents

Chapter 5
Managing Shared Directories

Chapter 6
Managing Shared Printers

Chapter 7
Managing Server Operations

Chapter 8
Sharing Processor Power

Appendix A: Managing Share-Level Security

Appendix B: The Server's lanman.ini File

Overview

This guide explains how to administer a local area network (LAN) server running the LAN Manager 2.2 Server Program. (The LAN Manager 2.2 Server Program incorporates version 2.2 of Microsoft® OS/2® LAN Manager technology.) It is intended for the administrator who will configure the LAN Manager Server Program installed on a computer running UNIX® System V Release 4.0 Version 2.1.

Some familiarity with the UNIX operating system (for the server) and with the MS-DOS and MS OS/2 operating systems (for clients) is assumed.

Depending on your level of experience and the task you want to perform, you will not need to read every page of this guide.

Chapter 1 describes the Server Program's features and capabilities and outlines the responsibilities of a LAN Manager administrator.

Chapter 2 provides information on the interfaces available for administering the LAN Manager software.

Chapter 3 outlines how to plan and initially configure a domain running user-level security and logon validation.

Chapter 4 describes how to create or manage user accounts and groups.

Chapter 5 details how to share directories and manage both shared directories and shared disks.

Chapter 6 describes how to share and manage printer queues.

Chapter 7 provides information on using various server administration features.

Chapter 8 describes how to share processing power via the Netrun service and by using distributed applications.

Appendix A outlines how to manage a server running share-level security.

Appendix B explains the LAN Manager configuration file on the server.

Appendix C describes the LAN Manager configuration file on the client (often called a workstation).

Appendix D outlines the NVAlert service.

Prerequisites for Administering LAN Manager

Before using this guide, you should already have performed the following tasks in the order listed:

1 Installed 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 Installed the LAN Manager 2.2 Server Program (hereafter referred to as the Server Program) on computers functioning as servers on the LAN. (For information about installing the Server Program, see the *LAN Manager Installation and Configuration Guide*.)

3 To make your administrative tasks easier, we suggest that you install the LAN Manager 2.2 Enhanced Client Program (hereafter referred to as the Client Program) on either an MS-DOS computer that is running Microsoft® Windows™ 3.0 or 3.1 and is connected to the LAN or on an MS OS/2 client on an MS OS/2 computer that is connected to the LAN. We recommend that you use this client to set up and administer the server. (For information about installing the Client Program, see the *LAN Manager Installation and Configuration Guide*.)

Conventions Used in This Guide

This guide uses the following typographical conventions to distinguish certain kinds of information:

- Text displayed on your screen is shown 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 like this:

  ```
  net use e:\\uname.serve\sharename
  ```

  Type characters shown in **boldface** exactly as printed; replace words shown in *italics* with text appropriate to your purpose. For example, to use the **net use** command to link to the *DOSUTIL* directory on a server named *buster*, type

  ```
  net use e:\\buster.serve\dosutil
  ```

  and press ↵.

  Optional input is enclosed in [square brackets]. For example, you can type the following command with or without specifying the name of a server:

  ```
  net print [\\uname.serve]
  ```

- Keys on your keyboard are shown like this: Ctrl.

  When you need to press two or more keys simultaneously, the key symbols are connected by a hyphen. For example, Ctrl - D indicates that you press Ctrl and D at the same time.

- The enter key is shown like this: ↵. If your keyboard does not have a key with this label, substitute the key used to send a carriage return.

- Screen labels for function keys, which are displayed at the bottom of the screen, are shown like this: HELP.

  Each screen label is associated with a specific function key — the first label on the left corresponds to F1, the next label corresponds to F2, and so on. The function keys are located on the left side or across the top of your keyboard. To use a screen label, press the associated function key on your keyboard.

- Do not use extended characters (other than 7-bit ASCII) in computer names, server names, share names, usernames or aliases. Doing so could cause some operations to fail.

Related Documentation

Because this guide makes reference to the following additional documents in the LAN Manager 2.2 Server package, it is recommended that you keep all of them at hand:

- *LAN Manager User's Guide for MS-DOS* introduces basic networking terms and concepts and provides procedures for accessing and using network resources from an MS-DOS based client.
- *LAN Manager User's Guide for MS OS/2* introduces basic networking terms and concepts and provides procedures for accessing and using network resources from an MS OS/2 based client.
- *Using LAN Manager with Microsoft Windows* provides instructions on how to log on and off, send and receive messages, and browse, connect to, and disconnect from network rewsources, all through Windows icons.
- *LAN Manager Troubleshooting and Command Reference* provides troubleshooting procedures, a list of error messages with recommended corrective actions, and a directory of commands for the Command Line Net Interface.
- *LAN Manager Installation and Configuration Guide* describes how to install the LAN Manager 2.2 software, and includes information for use with networks running earlier versions of the LAN Manager Server Program. This information serves three primary purposes:

  - It describes differences between the LAN Manager 2.2 software and earlier versions of the LAN Manager software.
  - It provides instructions for upgrading to the LAN Manager 2.2 software.
  - It discusses the considerations associated with temporarily using both types of software on the same network.

- *Remoteboot Guide* describes how to boot a client from a server with the remote boot feature.
- *SNMP Service User's Guide* describes how to install, operate and configure the SNMP server.
- *NetBEUI Transport Guide* describes how to install, configure, troubleshoot and tune the NetBEUI transport.
- *Multiprocessor Activator* explains how to set up LAN Manager servers using multiple microprocessors.

Chapter 1

Understanding LAN Manager

Overview

This chapter provides an overview of LAN Manager and the job of the administrator. It includes discussions of the following topics:

- features and services provided by the Server Program
- administrative tasks required for managing a LAN

Server Program Features and Services

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

Domains

To make it easier to manage a large or diverse network, LAN Manager lets you subdivide the network into administrative groupings of servers and clients, called ***domains***. Domains provide a simple way to control user access to the network, and they allow each user to work primarily with a specific set of servers and other users.

A network is typically divided into domains according to the way people work together — for example, the servers and clients in one department or on one floor might be grouped into one domain. A user can have accounts in multiple domains but can log on in only one domain at a time. When users view available servers, they see only servers in their own domain, not those on the whole network. However, they can still access resources on servers in any domain.

Dividing a large network into domains helps to keep it manageable, and intelligent use of domains can greatly simplify use of the LAN for both users and administrators.

Servernames

By default, all servernames for UNIX system LAN Manager servers end with the suffix **.serve**. Thus, LAN Manager servernames are in the form *uname*.**serve**, where *uname* is the UNIX system name of the server computer. Servernames must be eight characters or less in length.

For example, the servername for the server in the accounting department might be **acctng.serve**. The **.serve** suffix ensures that incoming calls from clients will be handled by the UNIX system Listener program. The Listener monitors the network, receiving and accepting incoming connection requests, and then invokes the service that is requested. It functions much like a telephone switchboard operator who answers a call, finds out who the caller wants to speak to, and then hands off the call to that destination.

Security

LAN Manager provides security features that let you control access to shared resources. A server can use either ***user-level security*** or ***share-level security***. Each server on the LAN must run one or the other level of security, and both user-level and share-level servers can coexist on the same LAN. The basic difference between the two security levels is in how they control access to the network and its shared resources:

- User-level security bases its control on a password associated with the user.
- Share-level security bases its control on a password associated with the resource.

User-Level Security

User-level security gives you precise control over access to shared resources. It also lets you take advantage of other LAN Manager security features, including logon validation (described later in this chapter).

Note: User-level security is the default. It is also the recommended security level. The focus of this guide is on administration of servers running user-level security. Many administrative tasks are identical for a server running either user-level or share-level security; Appendix A describes the differences in administering a share-level server.

Before sharing a resource on a server running user-level security, you set up a user account for each user who will be allowed access to the server. Under user-level security, only specified users can log on to the network. The username and password that a user supplies when logging on at a client are checked by a server to verify that they match those in a user account, and that the user is allowed access to the network.

Share-Level Security

On a server running share-level security, you assign a password and a single set of access permissions to each shared resource. Any user who can supply the password can use the resource, within the limits of the resource's access permissions.

Servers running share-level security can also be part of a domain running logon validation. A share-level server does not have a user accounts database, does not check the identity of users, and does not participate in logon validation. To use a resource on a share-level server, a user simply needs to have logged on to the network and to know the resource's password.

Other Security Methods and Features

In addition to designating user-level or share-level security for a server, you can take advantage of several other methods of protecting servers and network resources.

Activity Monitor. Some servers, such as those that share printer queues (described later in this chapter), may need to be physically accessible to many users. LAN Manager provides the ***Activity Monitor*** on the UNIX system console to protect these servers from unauthorized local access. The Activity Monitor provides a split-screen display of server and client activity, but does not allow access to the server's files. When starting the Activity Monitor, you can create a password that must be typed to unlock the keyboard. Users who do not know the keyboard lock password cannot exit from the Activity Monitor screen and access the server's files.

As an alternative to using the Activity Monitor, log off the server console when you will be away from it.

Hidden Servers. To protect a server from unauthorized remote access, you can hide it. ***Hidden servers*** are not shown when users view the list of servers in the domain. Users can still access the server and its resources if they know the server's name, but they have no way of using LAN Manager to find out that the server exists.

Password Encryption. When a user logs on to the network or requests access to a resource, his or her password is sent to a server for verification. Password encryption scrambles the user's password so that it remains secure while it is transmitted over the network.

Account Lockout. Accounts can be locked out after a specified number of failed logon attempts. This protects your network from unauthorized users who attempt to break into the network by using password generation schemes. Once an account is locked out, it is disabled until an administrator re-enables it. Lockout information is copied to all the servers in a domain.

Physically Secure Servers. Another way to protect servers from unauthorized local access is to isolate them physically in a locked room. You can use LAN Manager's remote administration feature (described later in this chapter) to administer these servers from any Enhanced MS-DOS or MS OS/2 client.

Security in Single-Server Domains. In a domain or network with only one server, there is no need to set up a domain-wide user accounts database for use by different servers. In a single-server domain, there are three options for setting up security:

- Set up the server to run user-level security and logon validation. This option is recommended to take advantage of the full range of LAN Manager security features.
- Set up the server to run user-level security without logon validation. A server set up in this way is called a ***standalone*** server. A standalone server checks usernames and user passwords only when users try to access resources.
- Set up the server to run share-level security.

Users and Groups

Under user-level security, each user who needs access to resources shared on a server must have a ***user account*** on that server. The user account, together with its associated password, identifies the user to LAN Manager. A user account can also include logon restrictions. For example, you can limit the hours during which the user can access the server's resources and the client computers from which the user can connect to the server.

For each user account, you assign ***access permissions*** for each resource you plan to share, defining the ways in which the user can use the resource. You can assign a different set of permissions for each user, and you can assign permissions differently for each shared resource. (These access permissions are applied in conjunction with the UNIX system permissions set for files and directories on the server. The interaction of these two kinds of permissions is described in Chapter 3.)

To simplify administration of user accounts, you can define ***groups*** of users and assign access permissions to a group. When you make a change to the attributes of a group — for example, by changing its permissions for a shared resource on a server — the change affects all users belonging to the group. You do not have to list each of the group's members individually.

Logon Validation

In a domain where at least one server is running user-level security, LAN Manager can validate users' requests to log on to the network and access network resources. ***Logon validation***, provided by the ***Netlogon service***, has two benefits:

- distribution of a domain-wide user accounts database
- control of access to the network by means of individual user passwords

Within a domain, all servers that run the Netlogon service keep identical copies of a single domain-wide ***user accounts database***. As administrator, you create and, when necessary, make changes to the user accounts database for the domain on only one server.

Administrative Resources

A server's ***administrative resources*** are used when network users and administrators perform certain tasks on the server, such as viewing shared resources, administering the server remotely, using the **netrun** command, and running distributed applications.

How a server's administrative resources are shared determines which of these tasks can be performed on the server. The administrative resources are hidden from most network users — only administrators can see them when viewing shared resources. There are three administrative resources:

- The ***ADMIN$*** resource controls access to server administration.
- The ***IPC$*** resource controls interprocess communication — that is, communication between different components of a program, different computers running parts of a single program, or two programs working together.
- The ***disk administrative resource, C$***, represents the server's UNIX system *root* directory. This resource is shared automatically whenever you start the server.

Only administrators can connect to the C$ resource. Doing so gives an administrator access to all directories and files on the server. An administrator working at a client cannot access a server's administrative resources unless *ADMIN$* and *IPC$* are shared.

File and Print Services

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

- The file service allows users, from their client computers, 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 connected to other computers on the network. These printers can be connected either directly to the server or to specially configured clients.

Shared Printer Queues

Servers can share ***printer queues*** to handle tasks for many users. A printer queue stores print jobs spooled from clients and sends them (usually in the order received) to printers as they become available. A printer queue can also send a file to an executable print processor script instead of to a printer. You can create a print processor script to manipulate a file in any way that suits your purposes.

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 MS-DOS clients. These ***shared client printers*** provide the following advantages:

- They increase the maximum number of network printers beyond the number of physical printer connections available on the server.
- They improve network flexibility by allowing client printers, shared among a common workgroup, to be installed in a location convenient to that group.

File Replication

File replication, provided by the ***Replicator service***, lets you maintain an identical, up-to-date set of directories and files on selected servers. Replication saves you the effort of updating files on many servers, spreads out the demand for heavily used files, and decreases the processing load on individual servers.

Messenger and Alerter Services

The server can send messages to clients running the ***Messenger service***. These messages pop up in a message window on top of most applications running on the client, or they can be sent directly to a log file. The user can either close a popup message window manually, with a single keystroke, or allow it to close itself automatically after a brief interval.

Some messages, including network error messages, resource status messages, and print job completion messages, can be generated automatically by the Server Program. As the administrator, you can also generate and send messages advising users of events on the system, such as an unscheduled server shutdown.

For more information on the Messenger service, see either *LAN Manager User's Guide for MS-DOS* or *LAN Manager User's Guide for MS OS/2*.

Under certain circumstances, such as when the file containing the server's audit trail is almost full, the ***Alerter service*** sends messages called alerts to a server or to a client running the Messenger service. On an MS OS/2 client, if the NetPopup service is running, the alert is displayed on the screen.

Audit Trail and Error Log

The ***audit trail*** is a tool for recording server resource usage. Available only on servers running user-level security, the audit trail provides the following information about each client-server link:

- the name of the server resource accessed
- the kind of operation performed or attempted
- the date and time of the operation
- the username requesting access

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 activity on the connection. For example, when a network user reads a file that is being audited, the initial read is recorded, but subsequent reads are not recorded.

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 per-project, for example, in an engineering or law firm.

LAN Manager keeps records of client and server errors in the server's ***error log***. On Windows clients, if the Messenger and WinPopup services are running and an error occurs, the WinPopup icon appears. Click on the icon to see the error message. On MS OS/2 clients, if the Messenger and NetPopup services are running, some errors also appear on the screen as alerts.

The error log displays the following information, listing errors in chronological order, from oldest to newest:

- service error
- error number
- date and time when the error occurred

You can view or clear the error log at any time.

Guarding Against Data Loss

LAN Manager can take advantage of the ***uninterruptible power supply*** (UPS) service, which performs an orderly shutdown to protect data in the event of a power failure. American Power Conversion Corporation (APC) sells UPS equipment (batteries, cables, associated software, and installation instructions) that has been certified to work with LAN Manager. The APC software interacts with LAN Manager by sending a notification message to all clients when a power failure has occurred. Contact APC at 1-800-788-2208 for ordering and pricing information.

Remote Administration

The Server Program allows you to administer the server from either an Enhanced MS-DOS or an MS OS/2 client, using either a windowed or a command line-oriented administration program. You can also administer the server by using the UNIX System Administrative Interface or the Command Line Net Interface. You can access these interfaces locally at the server's console, remotely from a client, or remotely via a UNIX system terminal session. The Kermit terminal emulator is supplied with the LAN Manager software for use in administering the server from a client. Kermit is only supported on the OSI protocol stack.

These administrative interfaces are described in Chapter 2.

Remote Booting

Clients can be booted remotely by a server using the Remoteboot service. For information on remote booting, see the *Remoteboot Guide.*

Netrun Service

With the Netrun service, users can run programs on a server from MS OS/2 clients. As an administrator, you decide how to set up the Netrun service, what programs to run with this service, and who can use the programs.

Text File Translation

The **ud** command enables users to translate ASCII text files from MS-DOS or MS OS/2 format to UNIX system format and vice versa. This allows a single text file to work with MS-DOS, MS 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 need for retraining. This feature is useful for network users who occasionally need to perform some tasks on the UNIX system and other tasks locally on clients.

For more information on the **ud** command, see either *LAN Manager User's Guide for MS-DOS* or *LAN Manager User's Guide for MS OS/2.*

The Administrator's Role

Administration of any network involves planning, designing, setting up, and maintaining the network. This section describes these responsibilities, dividing them into the following categories:

- planning the network
- administering the network

Planning the Network

Network planning tasks include the following:

- planning the division of the network into domains
- planning the configuration of each server within a domain
- evaluating and installing new applications and peripherals

The first step in setting up LAN Manager is to decide how you want the network organized. Once the hardware and software are installed on the computers on the network, you will share resources on servers and decide how to set up network security to control access. You will need to answer the following questions:

- How many servers and clients will the network have?

  There is no optimum ratio of servers to clients; the best ratio depends on the demands the users make on the network. Be sure to allow for future growth of the network.

- Which files, printers, or other resources do users need on a regular basis? How should these resources be distributed?

  Estimate the demand for these resources, and then think about how to spread them around the network to distribute the work load among servers.

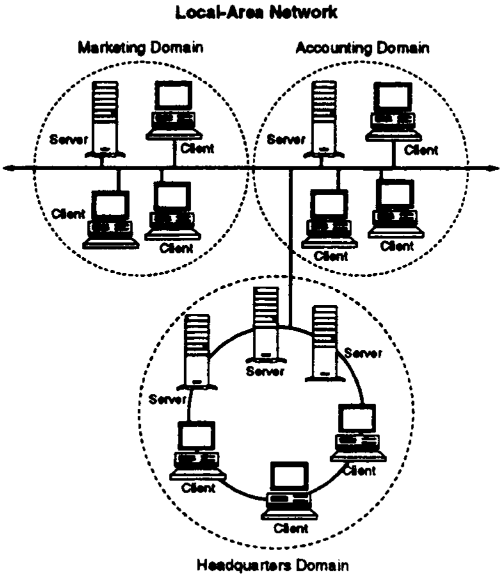
  Divide the network into domains if it is large or if users or computers fall into separate groups (for example, if your company has different divisions or work groups).

  Be sure to decide which servers will share resources, and which kind of security will be used at each server. Chapter 3 includes two worksheets to help you plan domains and set up servers.

- How secure do the network resources need to be? Can all users be allowed to use all resources? Should some resources, such as confidential files, be restricted, while other resources, such as printers, be available to all?

Figure 1-1 illustrates a sample network with three domains.

Figure 1-1: Network with Three Domains



Administering the Network

Once the network configuration is planned, administrative tasks include the following:

- initial configuration
- routine maintenance
- troubleshooting
- user education

Initial Configuration

Initial network configuration includes the following tasks, as a minimum:

- setting up the servers in each domain, including designating the primary domain controller and any backup domain controllers or member servers
- setting up the clients in each domain
- creating user accounts and groups on the primary domain controller and, if required, on any standalone servers
- sharing resources, including disk resources (directories) and printer queues

Routine Maintenance

Following are some of the routine day-to-day tasks necessary to maintain the network:

- keeping records of the network configuration
- adding new users and deleting users who no longer need access to server resources
- setting up shared directories
- installing application software (for more information, see the documentation provided with the application software)
- setting up and controlling shared printer queues
- controlling server disk storage space
- backing up and restoring server files

Troubleshooting

Certain less frequently performed tasks may be required to resolve 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 often not as straightforward as the routine tasks. However, aids and diagnostic tools are available to help you isolate and fix problems. Troubleshooting tasks are discussed in the *LAN Manager Troubleshooting and Command Reference*.

User Education

Educated users are crucial to a successful network. Following are some key tasks involved in educating network users:

- training new users
- communicating news about the network to all users
- providing help to all users
- maintaining a library of applicable documentation for all users

The lanman.ini Files

Each computer on the network, whether a server or a client, is initialized and configured by a file named *lanman.ini*, which is installed on the computer during installation of the LAN Manager software. As administrator, you control the way LAN Manager operates by interacting with servers' and clients' *lanman.ini* files.

- On a server, *lanman.ini* is installed in the *lanman* directory.
- On an Enhanced DOS client, *lanman.ini* is installed in the *lanman.dos* directory. On a Basic DOS client, *lanman.ini* is located in the *lanman.dos**basic* directory. On an MS OS/2 client, *lanman.ini* is located in the *lanman* directory.

Note: These are the default installation locations; they may have been installed elsewhere. If in doubt with regard to their locations, look at the **driver** lines in the *config.sys* file.

On both servers and clients, the *lanman.ini* file consists of a collection of ***keywords***, each with an associated value. Within the file, the keywords are grouped by function into ***sections***. Appendix B provides a complete reference to the server's *lanman.ini* file, and Appendix C provides a complete reference to the client's *lanman.ini* file. Each appendix lists all keywords by section, the range of acceptable values for each keyword, and the default value assigned during installation of the LAN Manager software.

This guide refers frequently to keywords in the server's *lanman.ini* file, and occasionally to keywords in the client's *lanman.ini* file. To adjust the configuration and operation of the LAN Manager software, you can change these keywords in the following ways:

On the server.

- Use the Net Admin Interface for Windows if you have an Enhanced MS-DOS client running Windows 3.0. This interface is described in Chapter 2 .
- Use the Net Admin Interface if you have an MS OS/2 client. This interface is described in Chapter 2.
- Use the UNIX System Administrative Interface. This interface is also described in Chapter 2.
- When logged in to the server's UNIX system at the server console, at a client running a terminal emulator, or at a remote terminal, use the **srvconfig** command. Use the following syntax to change keyword values in the server's *lanman.ini* file:

```
srvconfig -s section,keyword=value [ section,keyword=value ... ]
```

For each keyword to be changed, replace *section* with the name of its section, *keyword* with the name of the keyword, and *value* with the keyword's new value. Use spaces to separate multiple section/keyword/value arguments.

On the client. Use the Setup Program in the \lanman or \lanman.dos directory to reconfigure the client. For information on the Setup Program, see the *LAN Manager Installation and Configuration Guide*.

Chapter 2

Using the Administrative Interfaces

Overview

There are four interfaces available for administering LAN Manager servers:

1. **The Net Admin Interface for Windows** —a full screen, windows-based administration program available on Enhanced MS-DOS clients running Microsoft Windows. (A client is also often called a workstation.) To use this interface, you must have LAN Manager administrative privileges.
2. **The Net Admin Interface**—a full screen, menu-based administration program available on MS OS/2 clients. To use this interface, you must have LAN Manager administrative privileges.
3. **The UNIX System Administrative Interface**—a full screen, character-based, menu-oriented administration utility provided by the UNIX operating system. This interface is available at the server console, from a client on the LAN running a terminal emulator, or from a remote UNIX system terminal session. To use this interface, you must have root or administrative privileges on the server's UNIX system.
4. **The Command Line Net Interface**—a command-oriented interface. This interface consists of **net** commands that you can enter at an Enhanced MS-DOS or MS OS/2 client's system prompt, at the UNIX system prompt at the server console, at a client on the LAN running a terminal emulator, or at a remote terminal. To use this interface, you must have LAN Manager administrative privileges.

This chapter provides a detailed description of the Net Admin Interfaces and the UNIX System Administrative Interface. Most of the administrative procedures in this guide use the Net Admin Interfaces. Where the UNIX System Administrative Interface provides an alternative method for a given procedure, that alternative is shown as well.

You can also perform many administrative tasks using **net** commands through the Command Line Net Interface. However, it is recommended that until you gain experience administering LAN Manager, you use either the Net Admin Interface or the UNIX System Administrative Interface. This guide does not provide detailed instructions for using the **net** commands. Instead, after each procedure for which there is a corresponding **net** command, a summary of that command is given under the heading "Equivalent net Command." The **net** commands available to administrators are described more fully in the *LAN Manager Troubleshooting and Command Reference*. The **net** commands available to users are described in the *LAN Manager User's Guide for MS-DOS* and the *LAN Manager User's Guide for MS OS/2*.

When you begin administering a server running LAN Manager, you will probably feel more comfortable using the Net Admin Interfaces for most of your work.

When you have become familiar with the Server Program and want to start writing batch files to automate administrative tasks, you may find it more convenient to learn the command syntax of the Command Line Net Interface.

Using the Net Admin Interfaces

Using the Net Admin Interfaces, you can perform LAN Manager administrative tasks without having to memorize commands or command syntax.

This section provides instructions for the following tasks:

- starting the Net Admin Interfaces
- working with the screen
- changing the current focus
- logging off the network
- exiting from the Net Admin Interfaces

To perform administrative tasks from a client, you must begin by starting the Client Program.

Starting the Net Admin Interfaces

To start the Net Admin Interfaces, follow these steps:

1 At the client's system prompt, do *one* of the following:

   - If you have an Enhanced MS-DOS client, start your Windows environment and select the NetAdmin icon.
   - If you have an MS OS/2 client, do *one* of the following:

- Type **`net admin`** and press ↵.

  The system displays the LAN Manager screen with the focus on the client.

- Type **`net admin \\`***uname***`.serve`** and press ↵.

  Replace *uname* with the server's UNIX system name.

  The system displays the LAN Manager screen with the focus on the server. For an explanation of the current focus, see the section "Setting the Current Focus" later in this chapter.

Note: Typing **`net admin /mono`** for MS OS/2 clients improves the quality of the display on some monochrome computer screens. Try the command with and without **`/mono`** to determine which display you prefer.

If you are not currently logged on to the network, the `Log Onto Network` dialog box appears, with the following fields. Use the Tab key to move from one field to the next.

`Username`

This field is either populated with the value of the `username` keyword in the *[netshell]* section of the client's *lanman.ini* file or, if that keyword is blank, the field is blank.

Type over the entry in this field with a username with administrative privileges (such as the default, **`admin`**), or move to the next field if the existing entry is an administrative username.

`Password` Type the appropriate password for the username and move to the next field.

`Domain` Skip over this field to log on in the client's domain, or type in a different domain name.

2 Move to the `OK` command button at the bottom of the dialog box and press ↵.

A `Successful Logon` message box appears, showing the username you entered, the name of the server that verified your logon, the date and time you last logged on in the domain, and the time by which you must log off.

3 Press Esc or ↵.

For MS OS/2 clients, the following message should appear:

```
You have administrative privileges

at \\uname.serve
```

uname is replaced by the server's UNIX system name. If this message does not appear, exit and try this procedure again. For instructions, see the section "Exiting from the Net Admin Interfaces" later in this chapter.

For Enhanced MS-DOS clients, the privilege level appears automatically in the title bar of the LAN Manager screen.

4 Press Esc or ↵.

The Net Admin Interface screen appears. For a description of this screen, see the next section, "Working with the Net Admin Interfaces."

Equivalent net Command. You can skip the `Log Onto Network` dialog box in the previous procedure by logging on the network as an administrator before starting the Net Admin Interface. To do so, use the **net logon** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Working with the Net Admin Interfaces

The Net Admin Interface for Windows screen and the Net Admin Interface screen for MS OS/2 clients are similar. The Net Admin Interface screen for MS OS/2 clients is illustrated in Figure 2-1 and has the following elements:

a **Menu bar** — displays the names of menus from which you can choose commands.

b **Current focus** — for MS OS/2 clients, shows the name of your client or of the server that is the focus of activity when using the Net Admin Interface. For Enhanced MS-DOS Clients, the focus appears in the title bar.

c **Servers visible at the client** — a list of the computers in the domains visible to your client.

d **Client information** — provides the following information about your client:

`Your username` — the username you entered when you logged on to the network.

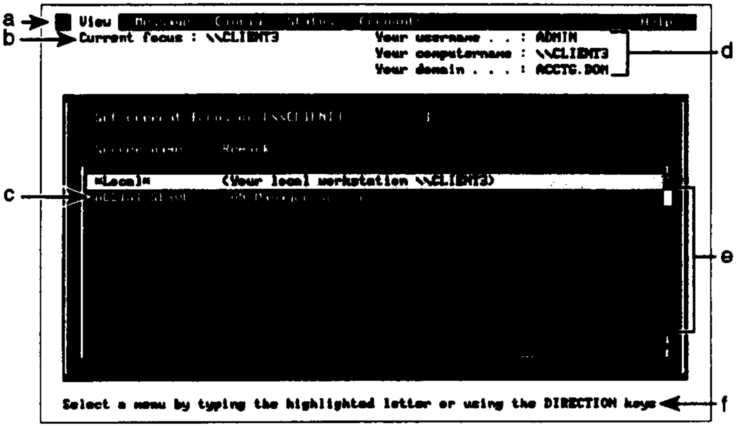
`Your computername` — the computername specified when the client was started.

`Your domain` — the domain name you entered when you logged on to the network. If you did not enter a domain name, you automatically logged on in the client's workstation domain, which is specified in the client's *lanman.ini* file. Note that the workstation domain and the logon domain are the same if you logged on in the workstation domain.

e **Scroll bar** — lets you use the mouse to scroll through the list box of servers.

f **Message line** — a brief statement about the current menu, command, or task.

Figure 2-1: Net Admin Interface Screen for MS OS/2 Clients



```
Current focus : \\CLIENT3          Your username . . : ADMIN
                                   Your computername : \\CLIENT3
                                   Your domain . . . : ACCTG.DOM

Set current focus on [\\CLIENT3        ]

Server name      Remark

*Local*          (Your local workstation \\CLIENT3)

Select a menu by typing the highlighted letter or using the DIRECTION keys
```

Using Menus

Menus are the starting point for any Net Admin Interface task. There are six available menus, the names of which appear in the menu bar across the top of the screen. To perform an administrative task, you select a menu, which displays a list of available commands. Except for `Exit` on the `View` menu, each command produces a dialog box, in which you enter information to perform the task.

Following are the six menus listed on the Net Admin Interface screen, and a summary of the tasks available through each menu:

Note: Individual menu options vary according to your focus. For example, if you have an Enhanced DOS client and your focus is on the server, you cannot view the client configuration.

`View` — View, control, and connect to resources shared by servers; view the connections of the client or server of current focus; view information about users on the network; exit from the Net Admin Interface.

`Message` — Send, log, and read messages; manage aliases (names used to receive messages).

`Config` — Log on, log off; use profiles; view the client configuration; set the server configuration; control services.

`Status` — View the status of shared resources; view client and server statistics and errors; read the audit trail and error log.

`Accounts` — Change user accounts and groups; view and set permissions and security settings for shared resources; change the options and password for your account at a server.

`Help` — Access on-line help.

You can work with menus using either the mouse or the keyboard, as follows:

- Using the keyboard, press Alt to activate the menu bar, then use the keys listed in Table 2-1.
- Using the mouse, select a menu for display by clicking on the menu name with the left mouse button. Select a command from the menu by clicking on the command's name.

Table 2-1: Using the Keyboard in a Menu

Key	Action
Letter keys	Select a menu or a command from a menu when the letter is highlighted in the name of the menu or command.
→ ←	Move from one menu name to another on the menu bar.
↓ ↑	Move from one command to another within a menu.
↵	Select a menu or a command.
Esc	Close a menu (remove it from the screen).

Using Dialog Boxes

Selecting a command from a menu displays a dialog box in which you enter information needed to perform the task selected. A dialog box, illustrated in Figure 2-2, contains one or more of the following kinds of fields:

a text boxes for entry of typed information

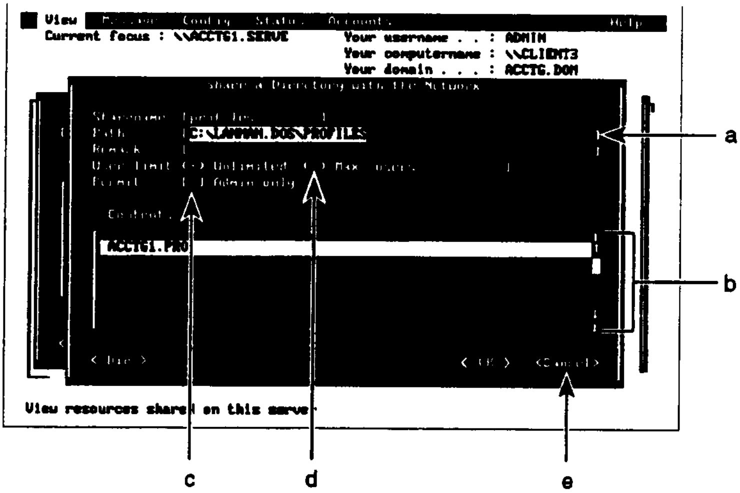
b list boxes with items to select from

c check boxes, in which you mark (select) or unmark (unselect) an item

d option buttons for selecting from among multiple options

e command buttons, which invoke an action

Figure 2-2: Dialog Box Fields



```
View  Message  Config  Status  Accounts                              Help
Current focus : \\ACCTG1.SERVE        Your username . . : ADMIN
                                      Your computername : \\CLIENT3
                                      Your domain . . . : ACCTG.DOM
                 Share a Directory with the Network

  Sharename   [profiles        ]
  Path        [C:\LANMAN.DOS\PROFILES                                ]
  Remark      [                                                      ]
  User limit  (•) Unlimited  ( ) Max. users      [    ]
  Permit      [ ] Admin only

   Contents :
  ACCTG1.PRO

  < Use >                                           < OK >  <Cancel>
View resources shared on this server
```

The following sections describe each of the field types included in a dialog box.

Use the keys listed in Table 2-2 to move around in a dialog box.

Table 2-2: Using the Keyboard in a Dialog Box

Key	Action
Letter keys	Move the cursor to the word with the letter highlighted. If the cursor is in a list or text box, you must hold down the Alt key while you press the letter key. The letter key corresponding to a letter highlighted in a command button selects that command button.
Tab	Move the cursor to the next field.
Shift - Tab	Move the cursor to the previous field.
↵	Perform the currently selected (highlighted) action.
Esc	Close the dialog box (remove it from the screen) and cancel any action selected.

Text Boxes. You type information in a text box. A text box is surrounded by square brackets and contains a line of dots that are replaced by characters as you type. Some text boxes can accept more characters than appear between the brackets; when you type past the right bracket, the contents of the text box scroll to the left. A text box may appear already filled with an entry, such as your username. In that case, press any character to erase the text box.

Use the keys listed in Table 2-3 to move around in a text box.

Table 2-3: Using the Keyboard in a Text Box

Key	**Action**
→	Move the cursor one space to the right.
←	Move the cursor one space to the left.
Home	Move the cursor to the first character in the text box.
End	Move the cursor to the last character in the text box.
Delete	Delete the character on the cursor.
Backspace	Delete the character to the left of the cursor.

Using the mouse, you can scroll the characters in a text box by clicking on a bracket with the left mouse button — the left bracket to scroll left and the right bracket to scroll right.

List Boxes. In a list box, you view items by scrolling through a list. For example, a list box might contain a list of resources available on a server or a queue of print jobs.

Use the keys listed in Table 2-4 to move around in a list box.

Table 2-4: Using the Keyboard in a List Box

Key	Action
↓	Move the highlight down one line.
↑	Move the highlight up one line.
Page Down	Move the highlight down one screenful of information.
Page Up	Move the highlight up one screenful of information.
Home	Move the highlight to the top of the list.
End	Move the highlight to the bottom of the list.
F5	Refresh the screen.
Letter keys	Move the highlight to the next item beginning with the letter pressed.

A scroll bar appears at the right of a list box, allowing you to use the mouse to move through a list with more items than can appear at once in the list box. Click on the up or down arrow with the left mouse button to move the view up or down one line. The position of the scroll box on the scroll bar indicates the relative position of the visible list box in the entire list. You can move through the list by positioning the mouse pointer on the scroll box, holding the left mouse button down, and dragging the scroll box up or down.

To use the mouse to select a list item, click on the item with the left mouse button. If the dialog box has a `Zoom` command button, you can zoom in on an item by double-clicking on the item with the left mouse button. Otherwise, double-clicking performs the action corresponding to the first command button listed.

Check Boxes. You use a check box to turn an option on or off. A check box, consisting of a pair of square brackets ([ ]), is marked with an `X` when the option is turned on and is empty when the option is turned off.

To mark or unmark a check box with the keyboard, use the spacebar as a toggle switch. To mark or unmark a check box with the mouse, click on the check box with the left mouse button.

Option Buttons. You use option buttons to select one option from among multiple options. One option button is always preselected, and only one option button can be selected at a time. An option button, consisting of a pair of parentheses ( ), is marked with a bullet (•) when it is selected.

To select an option button with the keyboard, use the keys listed in Table 2-5. To select an option button with the mouse, click on the option button with the left mouse button.

Table 2-5: Selecting Option Buttons

Key	Action
↓	Change the selected option to the next option.
↑	Change the selected option to the previous option.

Command Buttons. You use a command button to perform the action specified by the button. An active command button, specifying an available action, contains a highlighted letter. A command button that does not contain a highlighted letter is not active. Command buttons are displayed at the bottom of the screen and appear inside <angle brackets>.

You can select a command button from the keyboard in any of the following ways:

Press the Tab key to move to the command button, then press ↵.

If the cursor is not in a list or text box, press the letter key corresponding to the highlighted letter in the command button.

If the cursor is in a list or text box, hold down the Alt key while pressing the appropriate letter key.

To select a command button with the mouse, click on the command button with the left mouse button.

Using On-Line Help

The Net Admin Interfaces provide access to on-line help in two ways:

- To display information on the current menu, dialog box, or error message, press F1.

  A help screen appears. After reading it, select the `Done` command button or press the Esc key to close the help screen and return to the previous screen.

- To display information on a variety of LAN Manager topics, select the `Help` menu, then select a topic from the menu.
- The Net Admin Interface for Windows has a help button on each screen.

Equivalent net Command. You can also request help using the **net help** and **net helpmsg** commands. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Setting the Current Focus

If you have administrative privileges on a server, you can perform administrative tasks at that server using the Net Admin Interfaces from any Enhanced MS-DOS or MS OS/2 client on the network.

1 To administer a server, log on to the network using your username and password. Then do one of the following:

   - If you have an Enhanced MS-DOS client, start your Windows environment and select the NetAdmin icon to start a command processor for command-line administration or to start the Net Admin Interface for Windows at a client.

- If you have an MS OS/2 client, use the **net admin** command to start a command processor for command-line administration or to start the Net Admin Interface at a client.

The server you are administering must be sharing the *ADMIN$* and *IPC$* resources, which let you establish a session with the server. These resources are shared automatically when you start the server.

When you start the Net Admin Interface for Windows, the server's name appears in the titlebar.

When you start the Net Admin Interface on an MS OS/2 client, the `Current focus` line and the `Set current focus on` text box, by default, display the client's computername. This means that the client is the focus of activity when you use menus and dialog boxes.

2 To administer a server, you must set the current focus on that server. To do so, do *one* of the following:

- If you have an Enhanced MS-DOS client, do the following:

  — Type **`win netadmin`** and press ↵.

  The Net Admin Interface for Windows screen appears with the client's name in the titlebar.

- If you have an MS OS/2 client, do one of the following:

— Type **`net admin`** \uname.**serve** and press ↵. Replace *uname* with the server's UNIX system name.

The Net Admin Interface screen appears with the server's name on the `Current focus` line.

— Type **`net admin`** and press ↵.

The Net Admin Interface screen appears with the client's name on the `Current focus` line.

3 Follow these steps to change the current focus to the server:

a Select the servername by doing *one* of the following:

- Scroll through the list box of servers until the name appears and then press ↵.
- Press the first letter of the server's name until the name you want appears and then press ↵.

- Type the server's computername and then press ↵.

  (The server does not have to be listed for you to set the focus on it.)

b If you are prompted for a password, type the password needed to gain access to the server in the `Password` text box.

The Net Admin Interface screen shows the server of current focus and your privileges at that server.

Note: If you are administering servers from an MS OS/2 client, you can monitor several servers simultaneously by establishing different MS OS/2 sessions.

Example. Suppose you want to perform some administrative tasks on the *print2.serve* server down the hall. Rather than walk to the server, you want to administer it 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 password for *admin*).

You invoke the Net Admin Interface for Windows from your Enhanced MS-DOS client by starting your windows environment and selecting the NetAdmin icon.

You invoke the Net Admin Interface from your MS OS/2 client by typing **`net admin`** and pressing ↵.

From the Net Admin Interfaces, you change the current focus to `\\print2.serve.`

Note: By default, all servernames for UNIX system LAN Manager servers end with the suffix **.serve**. Thus, LAN Manager servernames are in the form *uname*.**serve**, where *uname* is the UNIX system name of the server computer. Servernames must be eight characters or less in length.

For example, the servername for the server in the accounting department might be **acctng.serve**. The will be handled by the UNIX system Listener program. The Listener monitors the network, receiving and accepting incoming connection requests, and then invoking the service that is requested. It functions much like a telephone switchboard operator who answers a call, finds out who the caller wants to speak to, and then hands off the call to that destination.

Logging Off the Network

When you log off the network, any resource sharing or connections you have established are canceled, but LAN Manager services are not stopped. As a security measure, log off when you will not be using the client for a while, so that no one else can use your network identity to share or use resources to which you have access.

To log off the network from the Net Admin Interfaces, follow these steps:

1. From the `Config` menu, select `Log off from LAN.`

   If you have any connections, the system displays a message regarding these connections and asks you to confirm your decision to log off.

2. Proceed according to the instructions on your screen.

After you log off, you cannot use any shared resources. However, the Workstation service is still running.

Equivalent net Command. You can also log off the network using the **net logoff** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Exiting from the Net Admin Interfaces

Exiting from the Net Admin Interfaces returns you to either the Windows application or the MS OS/2 prompt.

To exit from the Net Admin Interfaces, follow these steps:

1. Press Esc to close all dialog boxes until only the Interface screen is displayed.
2. Do *one* of the following:
   - Press Alt - F4.
   - Select the `View` menu, then select `Exit`.

If you are at an Enhanced MS-DOS client, the Windows application appears. If you are at an MS OS/2 client, the MS OS/2 prompt returns.

Using the UNIX System Administrative Interface

You can use the UNIX System Administrative Interface to administer the server software. Once you have installed the Server Program, the menu item `Lan Manager Server Administration` is added to the `Network Services Administration` menu. Using this menu selection, you can access the Server Program's `LAN Manager Server` menu, which in turn provides access to submenus and forms used to administer the Server Program.

This section describes how to access the UNIX System Administrative Interface and provides instructions for using the server UNIX System Administrative Interface features. You can perform these tasks from the server console or from a client on the LAN running a terminal emulator. For more advanced techniques, or for alternative ways of performing the same tasks described here, see your UNIX system administrator's guide.

If you are already familiar with the UNIX System Administrative Interface, skip to the section "Using Function Keys" later in this chapter for an explanation of the function keys that are specific to the Server Program. Then continue with the section "Assigning Root Privileges to the Server Administrator."

Throughout this section, references are made to arrow keys and function keys. If your keyboard does not have these keys, use the following alternatives:

If you do not have arrow keys, press Ctrl together with D to move the cursor down, U to move it up, R to move it right, and L to move it left.

If your keyboard does not have function keys, pressing Ctrl - F, followed by the number that corresponds to the desired function key may work.

If the display on your screen becomes garbled, press Ctrl - L to refresh the screen.

Accessing the UNIX System Administrative Interface

To access the UNIX System Administrative Interface, follow these steps:

Caution Only *one* person *should* use the UNIX System Administrative Interface at any given time; otherwise, data may be lost.

1 Log in as `root`.

2 At the UNIX system prompt (#), type **sysadm** and press ↵.

Note: Alternatively, you can type **sysadm LAN_Manager** and press ↵ to access the `LAN Manager Server` menu directly.

If the system prompts you for the **sysadm** password, type the password and press ↵.

The `UNIX System V Administration` menu appears.

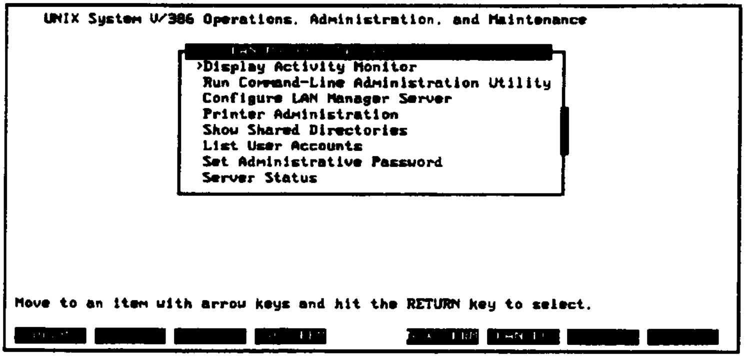
3 Move the cursor to `network_services` by typing **n** or using the arrow keys, then press ↵.

The `Network Services Management` menu appears.

4 Move the cursor to `LAN Manager Server` by typing **L** or using the arrow keys, then press ↵.

The `LAN Manager Server` menu appears, as illustrated in Figure 2-3.

Figure 2-3: LAN Manager Server Menu



```
    UNIX System V/386 Operations, Administration, and Maintenance

                          >Display Activity Monitor
                           Run Command-Line Administration Utility
                           Configure LAN Manager Server
                           Printer Administration
                           Show Shared Directories
                           List User Accounts
                           Set Administrative Password
                           Server Status

Move to an item with arrow keys and hit the RETURN key to select.
```

Using this menu, you can perform most of the administrative tasks for your server.

Working with the UNIX System Administrative Interface

The UNIX System Administrative Interface consists of screen displays called frames. A ***frame*** is a bordered rectangle containing a menu, a form, or text. As you move from frame to frame, each frame is numbered in sequence. Previous frames stay on the screen, inactive behind the current, active frame. The only time a frame is removed altogether is when you use the **CANCEL** function key.

Move from frame to frame as follows:

- To move forward, make a selection from a menu by using the arrow keys to move the cursor to the item you want, then pressing ↵.

  The next level of menu or form appears.

- To move back to the previous frame, do *one* of the following:

  — Press the CANCEL function key.

    The current frame disappears from the screen, and the previous frame becomes the active frame.

  — Press the PREV-FRM function key.

    The current frame becomes inactive, but stays on the screen behind the previous frame. The previous frame becomes the active frame.

Using Function Keys

Table 2-6 describes the screen labels for function keys that appear in the UNIX System Administrative Interface. To perform the action represented by the label, press the associated function key. Note that not every screen label appears on every screen.

Table 2-6: UNIX System Administrative Interface Function Keys

Screen Label	Action
CANCEL	Close the current frame and return to the previous frame.
CHOICES	Display all valid entries for the field where the cursor is positioned.
CONT	Perform the task indicated in the current frame.
ENTER	Select the item where the cursor is positioned.
EXIT	Exit from the current frame.
HELP	Access context-specific help. To scroll through the help message, use the arrow keys or the Prev Page and Next Page keys.
MARK	Select a menu item by marking it with an asterisk (*).
NEXT-FRM	Move to the next higher-numbered frame, when multiple frames are displayed. If the current frame is the highest-numbered, move to the lowest-numbered frame.
NEXTPAGE	Move to the next page, or text frame, in a report consisting of more than one page.
PREV-FRM	Move to the next lower-numbered frame, when multiple frames are displayed. If the current frame is the lowest-numbered, move to the highest-numbered frame.
PREVPAGE	Move to the previous page, or text frame, in a report

Table 2-6: *Continued*

Screen Label	Action
	consisting of more than one page.
RESET	Return the currently selected field to its original value.
SAVE	Save the information entered in a form and perform the task indicated.

Using Menus

When a menu appears on your screen, the cursor is initially positioned on the first menu item. To make a selection, do *one* of the following:

- Type the first letter of the item you want. If more than one item begins with the same letter(s), type the name up to and including the first unique letter. The cursor moves to the item. Press ↵.
- Use the arrow keys to move the cursor to the item you want, then press ↵.

To close a menu without making a selection, press the CANCEL function key.

Using Forms

Some menu selections produce forms. A form has one or more fields in which you must enter information about the task you want to perform.

When a form appears on your screen, the cursor is initially positioned on the first field. To complete the fields and perform the task represented by the form, follow these steps:

1 Use the arrow keys to move the cursor to the field you want to complete.

2 To enter information in the field, do *one* of the following:

   - Type a valid entry. To correct a typing error, backspace and retype.
   - Press the [CHOICES] function key.

     If there are more than two or three possible entries, a menu of entries appears. Move the cursor to the entry you want, then press ↵. The menu disappears, and the selected entry appears in the field.

     If there are only two or three possible entries, an entry appears in the field. Press [CHOICES] again to display the next choice. Continue until the entry you want appears.

     If you want to select more than one item from the list, use [MARK] and [SAVE].

     If there is no list of choices available, a message appears at the bottom of the screen informing you of that fact.

   When the field contains the entry you want, press ↵.

   The cursor moves to the next field.

3 When you have completed the form, press the [SAVE] function key.

   The system processes the information you entered and initiates the task associated with the form.

Exiting from the UNIX System Administrative Interface

To exit from the UNIX System Administrative Interface and return to the UNIX system prompt, do *one* of the following:

- From any menu or form, press Ctrl - J, then type **`exit`** and press ↵.
- Or follow these steps:
  - — From whichever menu you are in, press the CANCEL function key.
  - — Press EXIT.

The UNIX system prompt returns.

Logging In to the UNIX System with the Kermit Terminal Emulator

You can log in to the server's UNIX system and access the UNIX System Administrative Interface from a client by using a terminal emulator, such as Kermit. Kermit is installed in the server's *DOSUTIL* shared directory when the LAN Manager Server Program is installed. The following procedure is an example using Kermit.

Note: To log in to the UNIX system as *root*, you must log in at the server console. If you log in from a client using a terminal emulator or from a remote terminal, you must log in as a user and then use the **su** command to become *root*. (For information on the **su** command, see your UNIX system administrator's reference manual.)

To log in to the UNIX system, follow these steps:

1. Start the Client Program.
2. Log on to the network, supplying a valid username and its associated password.
3. Establish a link to the *DOSUTIL* directory and make that drive the current drive.
4. At the MS-DOS or the Compatibility Session of MS OS/2 prompt, type **`kermit`** and press ↵ to access the Kermit terminal emulator.

   The Kermit prompt, `MS-Kermit>`, appears.
5. Type **`set port net`** *uname* and press ↵.

Caution Do not use the **`.serve`** extension with *uname*. This may cause an error condition on the client.

Replace *uname* with the name of the UNIX system to which you want to log in.

The system displays a message stating that your nodename (the name of the client computer you are using) is being checked. The system then displays a message that the system is active.

6. Type **`connect`** (or just **`c`**) and press ↵.

   The system displays the Kermit terminal emulator screen, followed by the UNIX system login prompt.

Note: For instructions on switching back and forth between the UNIX and MS-DOS systems while using Kermit, see the next section.

7 Type a user login ID (other than `root`) and press ↵.

8 At the password prompt, type the appropriate password and press ↵.

9 Do *one* of the following:

- If a `TERM=` prompt appears, type **`kermit`** and press ↵.
- If the UNIX system shell prompt ($) appears, type **`TERM=kermit; export TERM`** and press ↵.

10 Follow these steps to become *root*:

a At the shell prompt, type **`su -`** and press ↵.

b At the password prompt, type the *root* password and press ↵.

To administer the Server Program, now access the `LAN Manager Server` menu, as described in the section "Accessing the UNIX System Administrative Interface" earlier in this chapter.

Temporarily Accessing the MS-DOS Prompt

When using Kermit, follow these steps to switch back and forth between the UNIX and MS-DOS systems:

1 At the UNIX system prompt, press Ctrl -] and then type **p** to return to the MS-DOS prompt.

2 At the MS-DOS prompt, type **`exit`** and press ↵.

The system prompts you to press the spacebar to continue.

3 Press Spacebar to return to the UNIX system prompt.

Exiting from the Kermit Terminal Emulator

To exit from the Kermit terminal emulator, follow these steps:

1 Use the exit procedure in the section "Exiting from the UNIX System Administrative Interface."

2 At the UNIX system prompt, press Ctrl -].

The information bar at the bottom of the screen disappears.

3 Type **`c`**.

The `MS-Kermit>` prompt appears.

4 Type **`exit`** and press ↵.

The MS-DOS prompt returns.

Chapter 3

Setting Up a Domain with Logon Validation

Overview

This chapter is designed to guide you through the planning and initial setup of a domain in which user-level security and logon validation will run — the most typical application of LAN Manager's capabilities. The chapter is organized as follows:

- Descriptions of the tasks required for planning a domain:
  - planning logon validation
  - planning user accounts and their attributes
  - planning groups
  - planning server security settings
  - planning resource access permissions
  - how user access is controlled
- Worksheets for initial planning, together with procedures for filling them out:
  - planning a domain
  - planning the configuration of an individual server within the domain
- Initial setup procedures:
  - designating the primary domain controller
  - designating a backup domain controller or member server
  - setting up a client

Planning Logon Validation

Each server running the Netlogon service has one of three roles:

- ***Primary domain controller*** — Each domain running logon validation must have one primary domain controller. The primary controller keeps the domain's ***master user accounts database***, and can validate logon requests in the domain.

  Note: You can change the user accounts database only on the primary domain controller.

- ***Backup domain controller*** — Each domain can have zero or more backup domain controllers. A backup domain controller keeps a copy of the domain's master user accounts database. Like the primary domain controller, a backup controller can validate logon requests. As a result, logon validation in the domain can continue even if the primary controller is unavailable.
- ***Member server*** — Each domain can have zero or more member servers. A member server keeps a copy of the domain-wide user accounts database, but it does not validate logon requests.

The Netlogon service ensures that each backup domain controller's and member server's copy of the domain-wide user accounts database is always identical to the master copy kept at the primary domain controller. At regular intervals, the primary controller sends each backup controller and member server database update information.

If the primary controller fails or is stopped, you cannot make changes to the domain's user accounts database, but logon request processing continues as long as one or more backup controllers are running in the domain. Because the primary, backup, and member controllers all keep their own copies of the database, and because the primary and all backups can validate logon requests, there is no single point of failure in the domain.

A server running user-level security without logon validation is called a standalone server. Each standalone server in a domain has its own user accounts database, which is administered individually and is not a copy of the master user accounts database.

Validation of Logon Requests

Running the Netlogon service on at least one server in the domain forces validation of users' logon requests. Each time a user logs on at a client in the domain, a logon request is sent to the domain's logon servers, the primary and backup domain controllers. If the user's account identifies a specific logon server, the logon request goes first to that server. If it is unavailable, another logon server (if there is one) will process the request.

The logon server that processes the request checks its copy of the domain-wide user accounts database for the username and password supplied in the logon request, and does one of the following:

- If the username and password match an account in the database, and the account's logon restrictions, if any, allow the user to log on at this hour and from this client, the user is logged on.
- If the username matches an account in the database but the password supplied does not match that account's password, or if the account is disabled or not allowed to log on at this time or at this client, the user is not logged on.
- If the username does not match an account in the database, the user is logged on as a standalone logon. The user is not logged on in the domain, and when an administrator views the list of users logged on in the domain, that username will not appear. The logon is not validated by any logon server and is separate from any domain on the network.

  A user logged on standalone cannot access the domain's servers that are running the Netlogon service, except by using a guest account. (See the section "The Guest Account" later in this chapter for details about guest accounts.) However, the user can access resources at standalone servers, servers running share-level security, or servers in other domains.

Note: In a domain not running logon validation, or a domain in which all the domain controllers are unavailable, all logon requests are processed as standalone logons.

Logon Validation and Earlier Versions of LAN Manager

Servers running versions prior to 2.0 of the Server Program can coexist in a domain with LAN Manager 2.2 servers. However, logon validation is not interoperable with versions earlier than 2.0. If the Netlogon service is running on any LAN Manager 2.2 server in the domain, each pre-2.0 server can run its version of the Netlogon service. When logon validation is running, each pre-2.0 server running user-level security in the domain has its own user accounts database and is treated as a standalone server. However, if a domain is running LAN Manager 2.2 logon validation, logon validation can be enforced for users at the domain's pre-2.0 client versions as well as those at LAN Manager 2.2 clients.

For information on setting up client scripts for pre-2.0 clients, see Chapter 4.

Planning User Accounts

Each user who needs access to resources shared on a server running user-level security must have a user account on that server. The user account identifies the user to LAN Manager.

If the domain is running logon validation, you must create user accounts on the primary domain controller for all users in the domain. The user accounts database is replicated on the domain's backup domain controllers and member servers; you do not create user accounts directly on any backup controller or member server. The user account is checked both when the user logs on in the domain and when the user requests access to shared resources.

If the domain is not running logon validation, you must create user accounts separately on each server running user-level security for users who need access to resources shared on that server.

Each user account must have a username and privilege level. You can also define more information for an account, including a password, operator privilege, logon restrictions, a logon script, a home directory, an expiration date, and group memberships. This section describes these attributes of a user account.

Relating LAN Manager Accounts to UNIX System Accounts

LAN Manager user accounts are related to UNIX system accounts. When you add a LAN Manager account, UNIX system accounts will be affected in one of the following ways:

- If a UNIX system account already exists by that name, add the LAN Manager account.

  Security checks, such as access to files, will depend on proper settings of the LAN Manager account **and** the UNIX system account. For example, if chriska tries to write to the *N:\PUBLIC\TEST.TXT* file (*/usr/public/test.txt* file on the server), he must have the following permissions:

  — W permission on *N:\PUBLIC.TXT* under LAN Manager, either by username or by group assignment.

  — w permission on */usr/public/text.txt* under the UNIX system, either as the owner ("u") or by chmod settings for "g" or "o". For example, `chmod o+w /usr/public/test.txt.`

- If a UNIX system account by that name does not already exist, add the LAN Manager account.

  LAN Manager automatically creates a UNIX system account by that name and gives the account the comment `.LAN Server .LMX` in the comment field of */etc/passwd*. You should **not** modify this comment unless you want to interfer with this functionality.

  Security checks will still depend on both the LAN Manager account and the UNIX system account, but it is assumed that you will not be assigning ownership or permissions under the UNIX system for this account since it didn't already exist prior to the addition of the LAN Manager account.

Therefore, the user will only be able to access resources that are allowed by the "o" bits of the UNIX system permission fields. LAN Manager permission settings are the recommended way to control access for this account.

When you remove a LAN Manager account, one of the following will occur:

- If the comment field in */etc/passwd* does not contain `.LAN Server .LMX`, the UNIX system account is left untouched. It is assumed that this account existed prior to the LAN Manager account.
- If the comment field in */etc/passwd* does contain `.LAN Server .LMX`, the UNIX system account is removed along with the LAN Manager account.

Note: Under some UNIX systems or security schemes, the UNIX system account may be locked instead of removed.

It is assumed that this account only existed as a convenience for LAN Manager operations. You should not assign ownership or permissions for this account locally under the UNIX system; when the account is removed, dangling UID references may remain in the file system.

Usernames

The username identifies the user to LAN Manager and to other network users. Each user account on the server must have a unique username.

Privileges

Each username has one of three privilege levels:

admin With admin privilege, the user can perform any administrative task on the server — start and stop services, create and modify user accounts, share resources, assign resource permissions, and manage printer queues. Admin privilege also includes user privilege, described later in this section.

Admin privilege includes access to all resources shared on the server, regardless of access permissions.

The default administrative account *admin* has admin privilege, and you can create additional accounts with admin privilege. When you delete an account with admin privilege, LAN Manager makes sure there is at least one other active account with admin privilege on the server, so that you will never delete the last administrative account and be locked out from administering the server.

When you install the server program, you are prompted to choose a password for the *admin* account.

Note: For security purposes, always assign a password to an account with admin privilege.

LAN Manager automatically puts all accounts with admin privilege into the special group *admins*.

user User privilege is the default privilege level and is the one you assign to most network users. User privilege allows use of network resources (subject to the access permissions for the resources), viewing of information about shared resources and the status of printer queues, and sending and receiving of messages.

LAN Manager automatically puts all accounts with user privilege into the special group *users*. This group is useful for assigning access permissions globally: to assign permissions for a resource to all users with accounts on the server (except those with guest privilege), assign those permissions to the *users* group.

You can also give an account with user privilege limited access to certain administrative functions by assigning operator privilege, as described in the next section.

guest Guest privilege is typically used to exclude temporary or occasional users from the permissions assigned to the *users* group.

LAN Manager automatically puts all accounts with guest privilege into the special group *guests*. An account with guest privilege cannot be assigned operator privilege.

Operator Privileges

An account with user privilege can also be assigned operator privilege, which allows the user to perform certain administrative tasks. A user can have one or more of three kinds of operator privilege:

server With server privilege, a user can

- share and stop sharing resources
- read and clear the error log
- close users' sessions and files that users have opened
- start and stop services
- view a list of all resources shared on the server

accounts With accounts privilege, a user can

- create, remove, and modify user accounts with user or guest privilege
- create, remove, and modify groups
- modify logon restrictions

Note: An accounts operator cannot modify an account with admin privilege except to change group memberships, and cannot change an account's privilege to admin.

print With print privilege, a user can

- share and stop sharing printer queues
- create, remove, and modify printer queues
- control print jobs
- view a list of all resources shared on the server (including admin-only resources)

Logon Hours

You can specify a range of logon hours for a user account, limiting the user's access to server resources to the days and times you specify.

You can also specify that if a user is using a resource at the server when his or her logon hours expire, the connection to the server is automatically terminated. Automatic termination is controlled by the security settings on the server, which are explained in the section "Planning Server Security Settings" later in this chapter.

The default value for logon hours allows the user to log on at any time.

Valid Clients

You can specify up to eight clients from which the user can access the server, or you can allow access from any client.

The default value allows the user access to the server from any client.

Logon Server

If the Netlogon service is running in the domain, you can specify which domain controller (the primary or one of the backups) is the user's logon server. If you specify a logon server, that server processes the user's logon requests. If the designated logon server is out of service when the user logs on, another domain controller will validate the logon request.

The default value allows any available server to process the user's logon request.

The Netlogon service can keep track of the last time a user logged on in the domain and the number of times the user has tried unsuccessfully to log on in the domain. This information can be accessed by an administrator.

Note: This record is kept only if you designate a specific logon server for the user.

When specifying logon servers for users, be sure to spread the logon processing load over all the domain's servers so as not to overload any one server by assigning too many users to it.

Logon Scripts

You can specify a ***logon script*** to be executed when a user logs on. A logon script is an executable or batch file of LAN Manager and/or operating system commands that runs on the client. It is typically used to configure the client for that user, performing such tasks as making network connections and starting applications. Scripts can be tailored for the requirements of each individual user.

For more information about logon scripts, see Chapter 4.

The default value for a user's logon script is none, that is, no script.

Home Directory

You can create a home directory on a server for a user, who can use that directory for file storage. If you assign a home directory, you can also limit the amount of disk space available to it. Using LAN Manager's **chkstor** command, you can monitor users' disk usage in their home directories.

For more information about the **chkstor** command, see the *LAN Manager Troubleshooting and Command Reference*.

The default value for a user's home directory is none, that is, no home directory.

Expiration Date

You can assign an expiration date to an account. The account is automatically disabled, but not removed from the database, on the assigned date. You can re-enable an expired account by removing the expiration date or assigning a new date.

The default value for an account expiration date is none, that is, no expiration date.

The Guest Account

LAN Manager installs a user account named *guest*, with no password, in the user accounts database of each server. You can use the guest account to provide access to resources on the server for users who do not have accounts on the server. When a user who has no account on a server requests access to a resource on that server, the user is allowed access according to the guest account's resource permissions.

One typical use of the guest account is to provide access to a server's shared printer queues.

Note: The server must have a guest account, which cannot have a password. If you assign a password to the guest account, you will need to modify lanman.ini keywords for the Replicator service. For more information, see Appendix B.

It is recommended that you assign guest privilege to the guest account. If you assign user privilege, the guest account becomes a member of the special group *users*, with all the resource permissions you have assigned to *users*.

Planning Groups

To simplify administration of user accounts, you can define groups of users and assign them groupnames. When you make a change to a group — for example, by assigning or changing resource access permissions — the change affects all users belonging to the group. You do not have to list each of the group's members individually.

Four groups are created automatically when the Server Program is installed:

- *users* consists of all non-administrative, non-guest user accounts on the server.
- *admins* consists of user accounts with admin privilege.
- *guests* consists of user accounts with guest privilege.
- *servers* consists of the servers in the domain.

You can create up to 252 groups in addition to these four. A group can consist of any number of users.

Each user can be a member of up to 253 groups: the 252 that you can define plus one of the *admins, users, guests* or *servers* groups, whose memberships are mutually exclusive.

Note: You can add individual users to a group, but you cannot add a group to other groups, that is, a group cannot be a member of another group.

You will typically create groups according to users' common interests — for example, a work group made up of individuals who perform the same kinds of tasks or functions, or users who need to use the same server resources.

Groups that you create on a domain's primary domain controller are copied to the backup domain controllers and member servers, just as user accounts and security settings are.

Planning Server Security Settings

The server's security settings define the rules for changing user account passwords on the server and how the server handles user logons outside of specified logon hours. There are six security settings:

Minimum password length specifies the minimum number of characters for a password. The range of values is from 0 (where passwords are not required for user accounts) to 14 characters. The default value is 6.

Password uniqueness prevents a user from re-using old passwords. The value you set is the number of previous passwords that are forbidden. For example, if you set a value of 3, a user is prevented from re-using any of his or her last three passwords. The range of values is from 0 (disabling the uniqueness requirement) to 8 passwords. The default value is 5.

Minimum password age is the minimum number of days that must elapse between password changes by a user. This restriction does not apply to administrators, who can change the password of a user at any time. The range of values is from 0 (disabling the minimum age requirement) to 49,710 days. The default value is 0.

Maximum password age is the maximum number of days that a user is allowed to use the same password without changing it.

The range of values is from 1 to 49,710 days, or unlimited. The default value is unlimited.

When you set the maximum password age for users in a domain, you are not setting an explicit expiration date. The time is counted from the day the password is changed, not from the day you set the value for maximum password age.

For example, suppose that on August 20, you set the maximum password age to 10. Any user who had not changed his or her password since August 10 would be allowed to log on one time and would receive a message that the password had expired. The user must change the password during that session in order to log on again. For example, those users who changed their passwords on August 19 would have their passwords expire on August 29.

Force logoff determines what happens if a user has a connection to a server when his or her logon hours or account expires. You can specify that the server will terminate the session immediately, terminate after a certain number of seconds, or not terminate. The range of values is from 1 to 11,574 seconds (slightly over 3 hours), immediately, or never. The default value is never.

The force logoff value affects only what happens when a user is already logged on. Regardless of this value, users are prevented from making a new connection to the server outside of their logon hours or after their accounts expire.

If force logoff is set to never, the user can continue to use existing connections until they log off, but cannot connect to any new network resources.

Lockout accounts specifies the maximum number of failed logon attempts users are allowed before their accounts are disabled. A failed logon attempt occurs when the user supplies an incorrect password when logging on.

If you aren't sure whether to use the lockout feature, or if you aren't sure how many attempts to permit, audit the system for failed logon attempts. If users are required to change passwords frequently, or if they use passwords that do not have simple mnemonics, legitimate users may routinely generate failed logon attempts. For more information, see Chapter 7.

By default, the lockout feature is disabled.

Security is more effective when users are forced to change passwords regularly. The maximum password age forces users to change passwords periodically. The minimum password age prevents a user from changing to a new password and then immediately changing back to the old one. Password uniqueness prevents a user from alternating between just a few passwords.

Security settings made on a domain's primary domain controller are copied to the domain's backup and member servers, just as user accounts and groups are.

Note: You can specify that a particular account is not required to have a password at all, using the **/passwordreq** parameter of the **net user** command. This parameter overrides the minimum password length security setting for that user only. For example, if a server's minimum password length is 8, you can use the **/passwordreq** parameter to specify that a given user account need not have a password. However, if the account does have a password, it must be at least 8 characters long.

Planning Resource Access Permissions

On the LAN Manager server, users and groups can be permitted or denied access to a resource.

A user who is not permitted to access a resource, either individually or as a member of a group, can link to that resource, but is unable to perform any other operations with it.

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

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 and 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.

For each shared disk and shared print queue resource on a server and for each user and group, you, as the administrator, must make these decisions about access permissions:

- Should you allow the specific user or group any access to the resource?

- Should you assign unique access permissions to each user or group that is allowed access to the resource? If so, what access permissions should you assign?

The next three sections describe access permissions for disk resources, printer queues, and named pipes.

Disk Resources

A disk resource is a disk drive, a directory, or a file. Following are the disk resource access permissions that you can assign to a user or group:

A (change attributes) Allows the user to change the MS-DOS or MS OS/2 file attributes — read-only, archive, hidden, or system. These attributes take precedence over LAN Manager access permissions.

C (create) Allows the user to create files and directories within the shared disk resource. Does not allow read or write access to existing files. (Each of these operations requires its own access permissions.) After creating a file, the user can read or write to that file only while it is initially opened. Once the file is closed, the user is unable to open it again.

D (delete) Allows the user to delete files and directories within the disk resource. Does not allow the user to delete the disk resource itself.

N (no)

Prevents the user from changing attributes, creating, deleting, and reading files or directories, and writing to files. When you assign the N permission, you cannot assign any other access permissions to the same user or group.

For disk resources, the N permission is sometimes indicated only by a colon (:).

Use this permission setting to exclude individual users from access despite their group memberships. For example, if you assign read and write permissions to the *users* group, you can exclude a specific user by assigning that user the N access permission.

P (change permissions)

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

You must set this permission on the file level; assigning P permission on a directory does not allow the user to set permissions on files within that directory.

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

R permission implies X permission, but X does not imply R. Therefore, if you assign R permission, you do not need to assign X permission as well. If you assign X without R, an MS OS/2 client can execute the file but cannot read it, while an MS-DOS client running a version of MS-DOS earlier than 5.0 can neither read nor execute the file.

For a user at an MS-DOS client to execute a program file (with a *.com*, *.exe*, or *.bat* extension), the user must have R permission for both the file and the directory containing it.

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

X (execute) Allows the user to open a file for execution.

Y (yes) An abbreviation for the ACDRW group of permissions.

MS OS/2 servers only — The Net Admin Interfaces provide convenient groupings of access permissions, so that you can easily assign common combinations of permissions. These commonly used combinations include RWX (read, write, and execute) and ACDR, create, delete, read, write, and execute).

Shared Printer Queues

A shared printer queue is a server resource that accepts print job requests, which are collections of data, such as files, that a user sends to a queue to be printed. A single server may have many shared printer queues sending print jobs to various printers that are either connected to the server directly or connected to other computers on the LAN. Once a user sends a print job request to a shared printer queue, he or she has no further interaction with the queue.

The Server Program lets you assign access permissions to groups and individual users for each shared printer queue. For each shared printer queue, you can assign one of the following access permissions to users or groups:

Y (yes)	The user can send jobs to the printer queue.
N (no)	The user cannot send jobs to the printer queue.
Y+P (yes + change permissions)	The user can send jobs to and set access permissions for the printer queue.

You can also assign default permissions for all printer queues. For additional information, see Chapter 6.

Note: When assigning permissions with the **net access** command, use Y or C (create) to represent the Y permission, N or a space to represent the N permission, and CP to represent the Y+P permission. (For a printer queue, permission to send a job is equivalent to permission to create a file.)

Named Pipes

Named pipes are used by some network applications for interprocess communication. A named pipe is used to send information between processes running different parts of an application, which may be on the same computer or on different computers. Refer to the documentation for your network applications to find the names of pipes they use.

You can assign permissions for named pipes to restrict the use of the applications that use those pipes. For each named pipe, you can assign one of the following access permissions to users or groups:

Y (yes)	The user can access the named pipe.
N (no)	The user cannot access the named pipe.
Y+P (yes + change permissions)	The user can access and set access permissions for the named pipe.

You can also assign default permissions for all named pipes. For additional information, see Chapter 6.

Note: When assigning permissions with the **net access** command, use **y** or **rw** to represent the Y permission, **n** or a space to represent the N permission, and **prw** to represent the Y+P permission. (For a named pipe, access permission is equivalent to permission to read and write to the pipe.)

How User Access Is Controlled

Permissions can be assigned to both users and groups, with one exception: N permission should not be assigned to a group. Use the N permission only to exclude a user from accessing a resource for which you have given access to a group to which the user belongs. For example, to allow all users except *kathy* to access the printer queue *laser*, assign Y permission to the group *users* and N permission to *kathy*.

If a user belongs to two groups, both of which are assigned permissions for a resource, then that user has all permissions assigned to both groups. For example, suppose the user *don* is a member of both *users* and *marketers*. If *users* has RW permission for the resource *reports*, and *marketers* has CW permission, then *don* has CRW permission.

If you assign permissions explicitly to a specific user, that user has only those permissions, regardless of the permissions assigned to any groups that include that user. For example, suppose the user *becky* is also a member of *users* and *marketers*, but you assign her only R permission for *reports*. In this case, the permissions for *reports* assigned to *users* and *marketers* are ignored for *becky*, who has only the permission you assigned to her explicitly.

Administrators at a server — that is, users whose accounts have admin privilege — can access all resources shared on that server, regardless of the access permissions set for those resources. Even if you assign an administrator N permission for a resource, he or she can still use the resource.

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

Figure 3-1 illustrates how a server running user-level security and logon validation decides whether a user should be allowed to log on to the network and use a shared resource. This decision depends on the following sequence of checks:

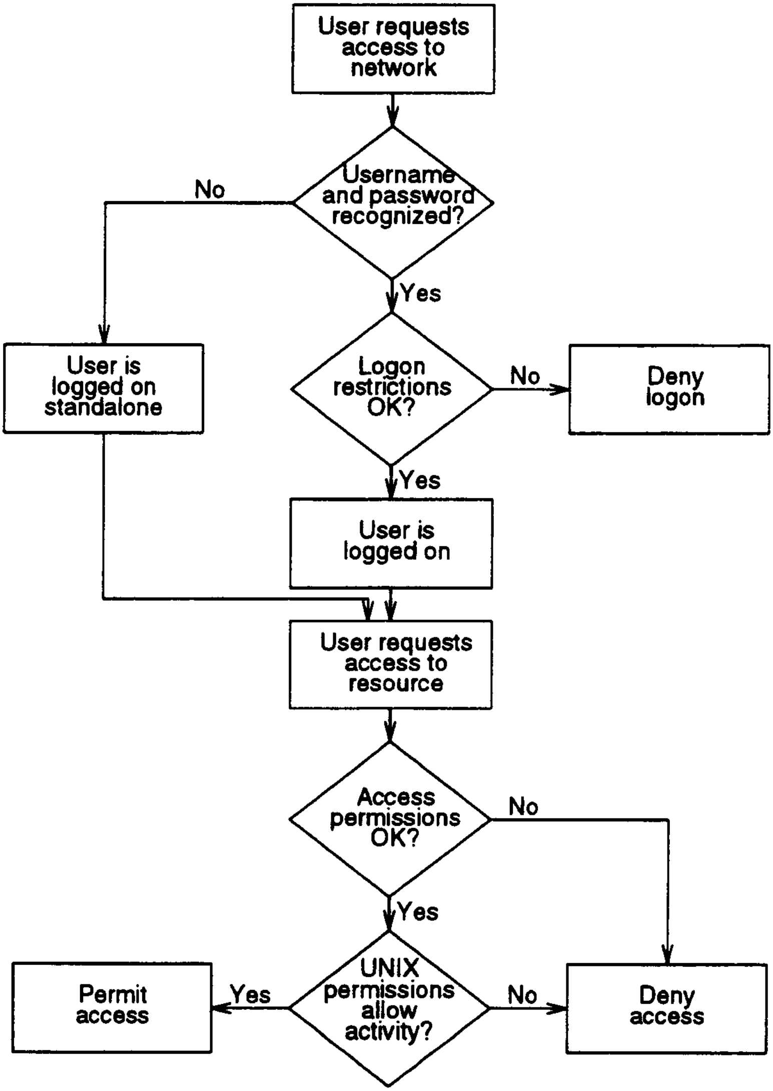
1. Do the username and password match an account in the user accounts database? If so, continue to Step 2. If not, log the user on as a standalone logon. A standalone user cannot access resources on a server running the Netlogon service, except by using a guest account.
2. Do the user's logon restrictions allow the request, that is, is the user allowed to log on from this client and at this hour? If so, log the user on to the network. If not, deny the logon request.

Once a user has logged on, his or her request to access a shared resource is subject to the following additional checks:

3 Do the access permissions set for the resource allow this user the requested access? If so, continue to Step 4. If not, deny access.

4 Do the UNIX system permissions set for the resource allow the requested access. If so, permit access. If not, deny access.

Figure 3-1: Determining Access to Resources on a Server Running User-Level Security


User requests access to network
Username and password recognized?
No
Yes
User is logged on standalone
Logon restrictions OK?
No
Deny logon
Yes
User is logged on
User requests access to resource
Access permissions OK?
No
Yes
UNIX permissions allow activity?
Yes
Permit access
No
Deny access

Using the Domain Setup Worksheet

This section provides a worksheet for planning logon validation within a domain, together with a procedure for filling out the worksheet. Before you begin, make a blank copy of the worksheet for each of the domains you have planned for your network.

This worksheet will help you decide how to configure a domain initially. Once the network is set up and running, it is easy to modify the configuration for performance or reliability, add new servers, change the roles of servers, or account for any other changes in the way the network is used. Once you have completed the domain worksheet, you may want to keep it on file for future reference.

The Domain Setup Worksheet helps you plan a domain with logon validation. Each numbered line on the worksheet corresponds to the step with the same number in the following procedure. Although the steps are numbered, they are not necessarily sequential.

Fill out the Domain Setup Worksheet as follows:

1 Assign a name to the domain.

2 Record the number of servers in the domain.

3 Record the number of clients in the domain.

4 Record how many servers of each kind, or role, will be included in the domain:

- There must be one primary domain controller.
- At least one backup domain controller is recommended; if enough servers are available, at least one controller per 50 users in the domain is recommended. For example, a domain with 200 users should have one primary and three backups, for a total of four.

  If there are no backups in the domain and the primary fails, all logon requests in the domain are processed as standalone logins.
- If you want a server to run user-level security using a different user accounts database from the domain-wide database, set it up as a standalone server.
- Servers that will not run logon validation will be either standalone servers with user-level security or servers with share-level security.

5 On another sheet of paper, list users who will need accounts in the domain-wide user accounts database, and consider how to divide them into groups. Each group should be made up of users with similar resource needs.

You can include up to 252 groups in the domain-wide database, in addition to the special groups *users*, *admins*, *guests*, and *servers*.

Assign each user a username and each group a groupname. Each name must be unique within the domain. Usernames and groupnames must conform to the following rules:

- A name can be up to 20 characters long.
- A name can include letters, numbers, and the following characters: ! # $ % & ( ) - . @ ^ _ ` { } ~

Names are case-insensitive. For example, *JOHN* is identical to *john*.

6 On your list of users, note which users will have administrative privilege, authorizing them to create and modify user accounts, start and stop services, share resources, and monitor network activity.

In addition, note which users will have operator privilege for the domain's servers. Operator privilege authorizes a non-administrative user to perform a subset of the administrative tasks. There are three kinds of operator privilege: server privilege, accounts privilege, and print privilege.

7 Decide whether to use logon scripts in the domain. If logon scripts will be used and more than one server in the domain will be validating logon requests, you will need to set up the Replicator service to maintain an identical set of scripts on each server.

For a description of logon scripts, see Chapter 4. For information about how to set up the Replicator service, see Chapter 7.

8 Record the computernames of the domain's primary domain controller, backup domain controllers, and member servers.

Domain Setup Worksheet

1 Domain name: ____________________

2 Number of servers in the domain: ____________________

3 Number of clients in the domain: ____________________

4 Number of each kind of server in the domain:

Primary domain controller ________1________

Backup domain controllers ____________________

Member servers ____________________

Standalone servers ____________________

Servers with share-level security ____________________

5 On another sheet of paper, list users who will need accounts in the domain's master user accounts database, groups of users that will need to be created, and groups that will need master database accounts. Give each user and group a unique name.

6 Note on the list in Item 5 which users will need administrative or operator privilege.

7 Will logon scripts be used in the domain?

Yes □ No □

8 List the servers that will run logon validation:

Primary	Backups	Members
____________________	____________________	____________________
	____________________	____________________
	____________________	____________________
	____________________	____________________
	____________________	____________________

Using the Server Setup Worksheet

This section provides a worksheet for planning security and resources for an individual server in a domain. Each numbered line on the worksheet corresponds to the step with the same number in the following procedure. Although the steps are numbered, they are not necessarily sequential.

Fill out the Server Setup Worksheet as follows:

1. Record the server's name.
2. Record the name of the domain that includes the server.
3. If logon validation will be running in the domain, record the name of the primary domain controller.
4. Record whether the server will run user-level or share-level security.
5. If the server will run user-level security, specify its role in the domain: primary, backup, member, or standalone.
6. On another sheet of paper, list the resources the server will share — for example, application software, directories, and printer queues — and note which users and groups will need access to those resources.

Assign each resource a sharename of up to 12 characters. (For clients running earlier versions of LAN manager to be able to access the resource, the last four of these characters must be a dot and a three-character extension.) A sharename should describe the shared resources it represents and should be easy to remember. For example, a shared printer queue for laser printers might be named *lasers*. However, a sharename does not have to be identical to the actual name of the shared resource. For example, word processing files might be kept on the server in a directory named */home2/lanman/wp*, but the directory's sharename might be *words*.

7 Decide which access permissions to set for the server's directories and files. Record these permissions on the list you made in Step 6. Permissions are set for users and groups, and apply to users working at the server itself.

If permissions for a particular file are not assigned to any users, then no users can even see that the file exists. Only administrators can see or access these files.

Server Setup Worksheet

1 Servername: ______________________________

2 Server's domain: ______________________________

3 If logon validation will run in the server's domain, which server is the primary domain controller?

____

4 What is the server's security mode?

User-level security □
Share-level security □

5 If the server is running user-level security, what is its role?

Primary domain controller □
Backup domain controller □
Member server □
Standalone server □

6 On another sheet of paper, list the resources the server will share, and note which users and groups will need access to each resource. Assign a sharename to each resource.

7 List important files on the server. For each file, note the access permissions that will be required for users and groups.

Designating the Primary Domain Controller

The first server to set up in a domain is the primary domain controller. The primary controller stores the master copy of the domain's user accounts database and, along with the backup domain controllers, validates users' logon requests.

Setting up the primary domain controller includes creating user accounts for the domain's backup controllers and member servers, as well as for the primary itself. LAN Manager uses these accounts when sending updates on the domain's user accounts database from the primary to the backups and members. Once you have set up these accounts, do not change or delete them. (If a server is removed from logon validation in the domain and no longer needs database updates, you can remove that server's account.)

If a single domain is to span multiple protocols and/or physical media, the recommended way to configure/administer the domain is to have the primary domain controller support all of the protocols and media. Other servers, functioning as either backup domain controllers or member servers, may then be scattered along each of the connected networks. Then, any administrative commands entered anywhere on the domain will be sent to the primary domain controller for processing, and the primary domain controller will forward the necessary updates along all of the protocols and media. Attempting to run a primary domain controller on one protocol with the backup domain controllers on a different protocol will create difficulties in file transfer and the backup domain controllers failing to receive administrative messages.

Ordinarily, you designate the first server you install as the primary domain controller during installation. To designate a primary domain controller after installation, you must use the Net Admin Interfaces, following these steps:

1. From the `Accounts` menu, select `Security settings.`

   The `Security Settings` dialog box appears.
2. In the `Role in domain` option buttons, select `Primary.`
3. Select the `OK` command button.
4. On MS OS/2 clients, the `Accounts` menu returns.

   Select the `Done` command button.

Equivalent net Command. You can also designate a primary domain controller after installation using the **net accounts** command with the **/role** parameter. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Designating a Backup Domain Controller or Member Server

Once the primary domain controller is set up and running, you can set up the backup controllers and member servers in the domain. Ordinarily, you designate each server's type during installation. To designate a backup controller or member server after installation, you must use the Net Admin Interfaces, following these steps for each backup and member:

1 From the `Accounts` menu, select `Security settings.`

  The `Security Settings` dialog box appears.

2 In the `Role in domain` option buttons, select *one* of the following:

  - `Backup` (for a backup domain controller)
  - `Member` (for a member server)

3 Select the `OK` command button.

4 For MS OS/2 clients, the `Accounts` menu returns.

  Select the `Done` command button.

Equivalent net Command. You can also designate a backup controller or member server after installation using the **net accounts** command with the **/role** parameter. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Changing a Server's Role

You can make changes to a domain's master user accounts database only by changing the database of the primary domain controller. All changes made to this database are copied automatically to the databases of the backup controllers and member servers. You cannot change the backup or member databases directly.

If you are not sure what a server's role is, use the **net accounts** command to check.

If the primary controller is stopped for some reason and you want to make changes to the domain's user accounts database, you can promote a backup or member to primary as described in the following procedure. Note that a change of this kind is subject to the following conditions:

- A domain can have only one primary controller. If the domain's primary controller is running, you cannot promote another server (change from backup to primary) without first stopping the existing primary.
- If you are switching the roles of the primary domain controller and another server, you must do so in three steps:

    1. Stop the Server Program on the current primary. For instructions on stopping and restarting the server, see Chapter 7.
    2. Change the role of the backup or member to primary, and start the Netlogon service on it.
    3. Change the old primary to its new role.

- For the Netlogon service to start for the first time on a server that has been demoted from primary to backup or member, the domain's new primary controller must be running.

- Changes to the domain's master user accounts database are not sent instantly to each backup controller and member server. Instead, updates are made at regular intervals, specified by the `pulse` keyword in the *[netlogon]* section of the primary's *lanman.ini* file. The default value of this keyword is 300 seconds (5 minutes).

  Note: If you have made changes just before the primary is stopped, the backups and members may not receive the update. If you then promote a backup or member to primary, these changes are lost.

- If you promote a backup or member to primary, you must change the role of the old primary to backup or member before you restart it. After restarting, its user accounts database will be updated by the new primary.

  Once you have started the old primary as a backup or member, and you are sure that its database is updated to match that of the new primary, you can, if desired, return these two servers to their former roles: change the new primary back to backup or member, then change the old primary back to primary again.

To be sure that the old primary's database is identical to that of the new primary before switching their roles, check the `pulse` keyword in the new primary's *lanman.ini* file. This keyword specifies how often (in seconds) the primary sends database updates to the domain's backups and members. If you know that this interval has passed since changes were last made to the database of the new primary, you can be sure the domain's other servers are up to date.

- If logon scripts are used in the domain, the primary controller must have a copy of them. Therefore, promoting a backup controller to primary requires less work than promoting a member server. Backup controllers should already have copies of the logon scripts. If you promote a member server, you must copy the scripts from one of the backup controllers to the member that you are promoting. For more information about how to set up a domain's logon scripts, see the next section.

To change the role of a server (primary, backup, member, or standalone) running user-level security in a domain running logon validation, use the procedure in either the section "Designating the Primary Domain Controller" or the section "Designating a Backup Domain Controller or Member Server" earlier in this chapter.

Dividing a Domain

You can reconfigure an existing domain by dividing it into two (or more) domains. This type of reconfiguration is often desirable when new computers are added to your network and your domains increase in size.

The following procedure explains how to divide an existing domain into two domains, promoting a backup domain controller from the first domain to the primary domain controller of the new domain. You can, of course, designate any server, whether existing on the old domain or newly added, as the primary domain controller of the new domain.

To divide a domain, follow these steps:

1. Make sure the server to be promoted has a copy of the user accounts database that is identical to that on the existing primary domain controller (that is, no user or group changes have occurred within the previous few minutes).
2. Stop the server to be promoted. (See "Stopping the Server Program" in Chapter 7.)
3. Change the selected backup domain controller's domain name to the name of the new domain as follows:

   a. At the UNIX system prompt, type **`sysadmin`** and press ↵.

      The `System Administration` menu appears.

b Select `network services.`

The `Network Services Management` menu appears.

c Select `LAN Manager Server.`

The `LAN Manager Server` menu appears.

d Select `Configure LAN Manager Server.`

The configuration screen appears.

e In the `Domain:` field, change the domain name to that of the new domain. (The three-character extension *.dom* is optional.)

4 Promote the former backup domain controller to the primary domain controller of the new domain. (See "Designating the Primary Controller" and "Changing a Server's Role" earlier in this chapter.)

5 If necessary, designate a new backup domain controller for the old domain. (See "Designating a Backup Controller or Member Server" earlier in this chapter.)

6 At the new primary domain controller, remove unwanted user accounts from the new domain. (See either the *LAN Manager User's Guide for MS-DOS* or the *LAN Manager User's Guide for MS OS/2*).

7 Change the domain names of any backup domain controllers and member servers that were moved to the new domain. (See Step 1 of this procedure.)

8 At the primary domain controller of the old domain, delete the user accounts of backup domain controllers and member servers that were moved to the new domain. (See either the *LAN Manager User's Guide for MS-DOS* or the *LAN Manager User's Guide for MS OS/2*).

9. Reconfigure any new computers as backup domain controllers or member servers in the old and/or new domain. (See the *LAN Manager Installation and Configuration Guide*.)

10. Change the domain name for each client in the new domain with the Setup Program, following these steps:

    a. Change to the *lanman* or *lanman.dos* directory as appropriate for your client type.

    b. At the MS-DOS or MS OS/2 system prompt, type **`setup`** and press ↵.

       The setup screen appears.

    c. From the Configuration menu, select `Workstation Settings`

       The Workstation Dialog box appears.

    d. In the domain text box, type the name of the domain and press ↵.

    e. Select the `OK` command button.

       On an Enhanced MS-DOS client, an additional dialog box appears for Windows support. Press ↵ to accept the default command button.

    f. From the LAN Manager menu, select EXIT.

    g. Reboot the client computer.

The domain is now divided into two domains, each with a primary and backup domain controller(s). Repeat this procedure for each domain you need to divide.

Chapter 4

Managing Users and Groups

Overview

After setting up a server running user-level security, your role as administrator is largely one of maintenance. You maintain user accounts and groups, making additions or changes as necessary. You also maintain shared resources, assigning access permissions whenever you share a new resource.

This chapter describes how to

- manage user accounts
- manage groups

Managing User Accounts

A user who wants access to resources on a server running user-level security must either have a user account with permission to access those resources or must be able to access the resources through the guest account.

This section provides procedures for the following user management tasks:

- adding user accounts
- cloning user accounts
- viewing and changing user passwords
- displaying and enabling existing user accounts
- removing user accounts

Adding a User Account

You will add user accounts to a server in the following circumstances:

- When you install a server.
- When you install a new client. (If the users who will use the client already have accounts on this server, you do not need to add any new accounts.)
- When a new user needs access to the server's resources.
- When you need to establish an anonymous account. You may sometimes need to create an account not identified with any particular individual, such as a guest printer account for people who need to use the

server only for occasional printing. It is usually safer to establish groups for this purpose; anonymous accounts are a potential security problem because it is hard to track the individuals who know the password and use the account.

Note: If you want a LAN Manager user account to be used also as a UNIX system account, add the account first through the UNIX system. One way to do this is through the UNIX System Administrative Interface. For more information about the interaction between LAN Manager and UNIX system accounts, see Chapter 3. You can also refer to your UNIX system administrator's guide.

Procedure. To add a user account to the server using the Net Admin Interface, follow these steps:

1 From the `Accounts` menu, select `Users.`

The `Select a User Account` dialog box appears, with a list box of existing user accounts.

2 Select the `Add user` command button.

The `Create a New User Account` dialog box appears.

3 In the `Account name` text box, type the username of the new account.

A username can be up to 20 characters long and can include letters, numbers, and the following characters: ! # $ % & ( ) - . ^ _ ` { } ~

4 In the Password text box, type a password for the user.

A password can be up to 14 characters long. The minimum length is specified in the server's security settings, as described in Chapter 3. For information on adjusting server security settings, see Chapter 7.

Advise each user to change his or her password after logging on for the first time.

Do not assign a null password to an account with admin privilege.

5 In the Full name text box, optionally type the user's full name.

6 In the Comment text box, optionally type a comment.

This comment will be displayed to an administrator viewing the list of users on the server. The user cannot change it.

7 In the User comment text box, optionally type a user comment.

This comment will be displayed to a user viewing the list of users on the server. The user can change it.

8 In the Country code text box, type the numeric code for the language in which the user's messages are to be displayed.

The default value is 001 (American English). See Table 4-1 for a list of the country codes. International versions of LAN Manager can be purchased separately.

9 From the `Privilege level` option buttons, select `Guest`, `User`, or `Admin`.

If you select `User`, you can optionally mark one or more of the `Operator privileges` check boxes, `Server`, `Accounts`, and `Print`, to give a user with user privilege the ability to perform certain kinds of administrative tasks. (The `Comm` check box is not applicable to LAN Manager for UNIX system servers.)

For a description of privileges, see Chapter 3.

10 To add the user to one or more existing groups, select the `Groups` command button.

The `Group Memberships for User` dialog box appears. To assign group memberships now, turn to the procedure "Assigning Group Memberships," then return to this step of this procedure.

11 To limit the hours when the user can access the server, specify which clients the user can use, and/or give the account an expiration date, select the `Logon` command button.

The `Logon Restrictions for User` dialog box appears. To assign logon restrictions now, turn to the procedure in the section "Assigning Logon Restrictions" later in this chapter, then return to this step of this procedure.

12 To assign the user a logon server, logon script, and/or home directory, select the `Paths` command button.

The `Set Paths for User Account` dialog box appears. To set paths now, turn to the procedure in the section "Setting Paths" later in this chapter, then return to this step of this procedure.

13 Select the `OK` command button.

The `Create a New User Account` dialog box returns.

14 Windows — Select the `OK` command button.

MS OS/2 — Select the `Done` command button.

Equivalent net Command. You can also add a user account to the server using the **net user** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Table 4-1: Country Codes

Country	Code	Country	Code
Asia	099	Latin America	003
Australia	061	Netherlands	031
Belgium	032	Norway	047
Canada	002	Portugal	351
Denmark	045	Spain	034
Finland	358	Sweden	046
France	033	Switzerland	041
Germany	049	United Kingdom	044
Italy	039	United States	001
Japan	081		

Note: The language you select will appear only if the appropriate international version of LAN Manager is loaded on your server. International versions of LAN Manager may be purchased separately.

Assigning Group Memberships

To assign group memberships when you are adding a new user account, follow these steps:

1 In the `Create a New User Account` dialog box, select the `Groups` command button.

The `Group Memberships for User` dialog box appears, with two list boxes:

`Member of`	shows the groups to which the new user belongs.
`Not a member of`	shows the groups to which the user does not belong.

2 To add the user to a group, in the `Not a member of` list box, move the highlight to the name of the desired group, then select the `Join` command button.

The selected groupname moves to the `Member of` list box.

Repeat this step until the user is added to as many groups as needed.

3 To remove the user from a group, in the `Member of` list box, move the highlight to the name of the desired group, then select the `Leave` command button.

The selected groupname moves to the `Not a Member of` list box.

Repeat this step until the user is removed from as many groups as needed.

To remove the user from all groups except the groups to which he or she is automatically assigned (*admins*, *users*, or *guests*), select the `Leave all` command button.

4 Select the `OK` command button.

5 Return to Step 10 of the "Adding a User Account" procedure.

Assigning Logon Restrictions

To assign logon restrictions for a user account, follow these steps:

1 Do *one* of the following:

- If you are adding a new user account, in the `Create a New User Account` dialog box, select the `Logon` command button.
- If you are administering an existing user account, follow these steps:

  a From the `Accounts` menu, select `Users.`

  The `Select a User Account` dialog box appears.

  b In the list box of user accounts, move the highlight to the user name you want, then select the `Zoom` command button.

  The `View the User Account` dialog box appears.

c Select the `Logon` command button.

The `Logon Restrictions for User` appears.

2 To set an expiration date for the account, in the `Account expires` text box, type a date and/or time.

LAN Manager accepts all of the following formats for the expiration date:

```
7-23-92
7-23-92 8am
7/23/92 5 pm
7-23-92 8:00
7-23-92 17:30:32
```

To set no expiration date, leave the `Account expires` text box blank.

3 To specify the clients at which a user can log on, in the `Valid workstations` option buttons, do *one* of the following:

- Select `Any workstation` to allow the user to log on at any client.
- Select `Listed` to limit the clients at which the user can log on. In the adjacent text box, type the computernames of up to eight clients.

4 To specify the times when the user can log on, adjust the graph under `Hours logon allowed` as follows:

- To clear all logon hours on an MS-DOS client, press the `Clear all` command button. To clear all logon hours on an MS OS/2 client, press the `Clear` command button.

- To allow the user to log on at all times do one of the following:
  - — If you are at an MS-DOS client, press the `Permit All` command button.
  - — If you are at an MS OS/2 client, press the `Permit all hours` command button.

  This is the default value.
- To allow or prevent use at a specific hour, move the cursor to that hour on the graph and press the spacebar, or click on that point with the left mouse button.

5 Select the `OK` command button.

6 Do *one* of the following:

- If you are adding a new user account, return to Step 11 of the "Adding a User Account" procedure.
- If you are administering an existing user account, the `Select a User Account` dialog box returns. Select the `Done` command button.

Setting Paths

To specify a logon server, logon script, or home directory for a user account, follow these steps:

1 Do *one* of the following:

- If you are adding a new user account, in the `Create a New User Account` dialog box, select the `Paths` command button.

- If you are administering an existing user account, follow these steps:

  a From the `Accounts` menu, select `Users.`

  The `Select a User Account` dialog box appears.

  b In the list box of user accounts, move the highlight to the user name you want, then select the `Zoom` command button.

  The `View the User Account` dialog box appears.

  c Select the `Paths` command button.

  The `Set Paths for User Account` dialog box appears.

Note: Use this dialog box only if you are adding the account to a domain's master user accounts database or administering an existing account in the database.

2 To assign the user a logon server, in the `Logon server` option buttons, do *one* of the following:

- Select `Domain controller` for logon processing by the primary domain controller. (If the primary is unavailable, a backup domain controller will process logon requests, if the domain has backup controllers.)

- Select `Any server` for logon processing by any available logon server. This is the default selection.
- Select `Servername` to specify a logon server. In the adjacent text box, type the computername of a backup controller to have that backup process the user's logon requests. (If the specified controller is unavailable, the primary or another backup will process logon requests.)

3 If the user has a logon script, identify it by typing its filename or path in the `Logon script` text box.

For a user of a LAN Manager 2.0 or later client, the logon script path is relative to the value of the `scripts` keyword in the *[netlogon]* section of the logon server's *lanman.ini* file.

For a user of a client running an earlier version of LAN Manager, the logon script path is relative to the logon server's */usr/net/servers/lanman* directory.

4 To assign the user a home directory, follow these steps:

a Type the name of the home directory in the `Home directory` text box.

The name can be an absolute pathname (for a home directory on the primary domain controller) or a Universal Naming Convention (UNC) name in the form \uname.**serve***sharename*, where *uname* is the server's UNIX system name and *sharename* is the home directory's sharename. If the directory does not exist, LAN Manager prompts you to confirm that you want to create it.

Note: You can specify a default location for all users' home directories by changing the value of the `userpath` keyword in the *[server]* section of the server's *lanman.ini* file.

b To specify the size of the user's home directory, in the `User storage limit` option buttons, do *one* of the following:

- Select `None` (the default) for no limit.
- Select `Maximum` to set a size limit. In the adjacent text box, type the limit (in KBytes).

  If the user exceeds this limit, LAN Manager will send an alert to both the user and the administrator when you use the **chkstor** command. If no user exceeds the limit, LAN Manager will not send an alert or any other message. (For more information about the **chkstor** command, see the *LAN Manager Troubleshooting and Command Reference*.)

Note: You must also assign the user ACDPRW permissions for the user's home directory. For instructions on assigning permissions for a directory, see Chapter 5.

5 Select the `OK` command button.

6 Do *one* of the following:

- If you are adding a new user account, return to Step 12 of the "Adding a User Account" procedure.
- If you are administering an existing user account, the `Select a User Account` dialog box returns. Select the `Done` command button.

Equivalent net Command. You can also specify a logon server, logon script, or home directory for a user account using the **net user** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Cloning a User Account

You can also create a new user account by cloning, or using an existing user account as a template for the new account. You can save effort by using this method, because the new account duplicates all information from the existing account except for the account name, full name, and password. You can then change only those account attributes that you want to be different, such as the identity of the new user's home directory.

Note: You can clone an account only through the Net Admin Interface; there is no equivalent command-line command.

To clone a user account using the Net Admin Interface, follow these steps:

1 From the `Accounts` menu, select `Users`.

The `Select a User Account` dialog box appears.

2 In the list box of existing user accounts, move the highlight to the name of the account to serve as the template, then select the `Clone` command button.

The `Create a New User Account` dialog box appears. All text boxes contain the information on the existing account, except for `Account name`, `Password`, and `Full name`.

3 In the `Account name` text box, type the username of the new account.

4 In the `Password` text box, type a password for the user.

5 In the `Full name` text box, optionally type the user's full name.

6 Follow Steps 6 through 12 of the "Adding a User Account" procedure earlier in this chapter to customize the account for this user.

If the existing account serving as the template has a home directory, be sure to change that option for the new account.

7 Select the `OK` command button.

The `Select a User Account` dialog box returns.

8 Windows — Select the `OK` command button.

MS OS/2 — Select the `Done` command button.

Viewing and Changing a User Account

When you view a user account, LAN Manager can report information about the user's use of a password and logon requests, in addition to the account information you specified initially.

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

- when a user forgets his or her password
- when a user fails to change his or her password for a long time
- when you need to force a password change for security reasons

Once the password has been changed, the new password is automatically updated on all servers in the same domain.

Procedure. To view or change information about a user account using the Net Admin Interface, follow these steps:

1 From the `Accounts` menu, select `Users.`

  The `Select a User Account` dialog box appears.

2 In the list box of user accounts, move the highlight to the name of the desired account, then select the `Zoom` command button.

The `View the User Account` dialog box appears, with the account information you have specified for this user. In addition, the following information is displayed:

- when the user last logged on in the domain

  Note: This server will only record logons validated by this server. To ensure the accuracy of this statistic, the user must always log on to this server. To designate a specific logon server, see "Setting Paths" earlier in this chapter.

- how many times the user has tried unsuccessfully to log on in the domain (if this account is in a domain's master user accounts database)
- when the user last changed his or her password
- when the user will next be allowed to change his or her password
- when the user's password will expire

The information in the `Password Last Changed` field may be inaccurate and should be ignored.

Note: If this account is in a domain's master user accounts database, the date and time the user last logged on in the domain and the number of unsuccessful logon attempts are also displayed. However, this information is accurate only if a specific logon server is designated for this user. (The dialog box displayed when you select the `Paths` command button shows whether a logon server is specified for the user.)

In addition, the date of last logon and the number of unsuccessful logon attempts do not reflect any logon attempts by the user from clients running LAN Manager earlier than 2.0.

3 To change any of the account information that you have specified for this user, type over the appropriate text box, change the option button selected, and/or change the check boxes marked.

You cannot change the information in the `Last logon`, `Failed logon count`, `Password last changed`, `Next change available`, and `Password expires` text boxes.

To change the user's password, which is not displayed, type a new password in the `Password` text box.

You can also select the `Groups`, `Logon`, and/or `Paths` command buttons to change any of the information in the associated dialog boxes for the account.

4 Select the OK command button.

The Select a User Account dialog box returns.

5 Windows — Select the OK command button.

MS OS/2 — Select the Done command button.

Equivalent net Command. You can also view or change information about a user account using the **net user** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Disabling or Re-enabling a User Account

Disabling a user account prevents the user from logging on; it does not delete the account from the server's user accounts database. The account-disabling feature lets you maintain generic accounts for use as needed, such as for cloning. You can also temporarily disable an account, for example, while a user is on vacation.

Also, accounts are automatically disabled, or "locked out," when users exceed the maximum allowable number of failed logon attempts. When an account is locked out, you must re-enable it to allow further logons. By default, the lockout feature is turned off. See Chapter 7 for information on turning on the lockout feature.

To disable or re-enable a user account using the Net Admin Interface, follow these steps:

1 From the Accounts menu, select Users.

The Select a User Account dialog box returns.

2 In the list box of user accounts, move the highlight to an account name, then select the Zoom command button.

The `View the User Account` dialog box appears.

3 Do *one* of the following:

- To disable the account, mark the `Disable account` check box.
- To enable the account, unmark the `Disable account` check box.

4 Select the `OK` command button.

The `Select a User Account` dialog box returns.

5 Windows — Select the `OK` command button.

MS OS/2 — Select the `Done` command button.

Equivalent net Command. You can also disable or re-enable a user account using the **net user** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Deleting a User Account

You may need to delete a user account under any of the following circumstances:

- when you change an account's 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 a specific server
- when you must close the account for security reasons

When you remove a LAN Manager account, you may affect the UNIX system accounts. For more information on the interaction between LAN Manager and UNIX system accounts, see Chapter 3.

You can temporarily disable a user account without deleting it. When an account is disabled, the user cannot access server resources. See the previous section for information on disabling a user account.

Procedure. To delete a user account, follow these steps:

1 At the console, copy any files to be saved from the user's home directory to another directory.

2 At the console, remove the user's home directory.

3 At your client, using the Net Admin Interface, from the `Accounts` menu, select `Users`.

   The `Select a User Account` dialog box appears.

4 In the list box of user accounts, move the highlight to the name of the account to be deleted, then select the `Delete` command button.

   A request for confirmation appears.

5 To confirm, select the `OK` command button.

   The `Select a User Account` dialog box returns.

6 Windows — Select the `OK` command button.

   MS OS/2 — Select the `Done` command button.

Equivalent net Command. You can also delete a user account using the **net user** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Using the UNIX System Administrative Interface to Manage User Accounts

To add a user account, view or change information about an account, or delete an account using the UNIX System Administrative Interface, follow these steps:

Caution Only *one* person should use the UNIX System Administrative Interface at any given time; otherwise, data may be lost.

1. Access the `LAN Manager Server` menu, as described in Chapter 2.
2. Select `List User Accounts.`

   The system displays the `User Accounts` frame, listing LAN Manager accounts and their corresponding UNIX system accounts.
3. Press the CANCEL function key to return to the `LAN Manager Server` menu.
4. Add, change, or delete user accounts using the Command-Line Administration Utility. For instructions on using this utility, see Chapter 7.

Specifying Common User Startup Operations

In a domain running logon validation, you can specify logon scripts to be run on the client when a user logs on in the domain. A script can be a batch file or an executable file, and typically consists of commands to make network connections and/or start applications.

For example, the following batch file, which makes two network connections and starts Microsoft Excel, might be used as a logon script:

```
net use d: \\product.serve\accountfiles
net use lpt1: \\product2.serve\laser
excel
```

You can create a single script for all users in a domain or a different script for each user. Each user's account specifies the name of the appropriate logon script, if any, and the script is run each time that user logs on in the domain.

Scripts are kept on primary and backup domain controllers. When a user logs on, LAN Manager checks the user's account on the logon server for the name of a script. The *[netlogon]* section of each server's *lanman.ini* file has a `scripts` keyword identifying the directory containing the server's logon scripts. The value of this keyword can be either a pathname relative to the *lanman* directory or an absolute pathname. The default value is `/var/opt/lanman/repl/import/scripts`. When you install a primary domain controller, the value is automatically changed to `/var/opt/lanman/repl/export/scripts`.

For a user's logon script to run, the following conditions must be met for the user to have access to the script:

- The *scripts* directory must be shared.
- The user must have R (read) permission for the script.

Assign the appropriate permissions on the directory in which the scripts reside to all users who will be using the scripts.

LAN Manager automatically provides this access. When the Netlogon service starts, LAN Manager shares the directory identified by the `scripts` keyword with the sharename *NETLOGON*. LAN Manager also assigns RX (read and execute) permission for the *scripts* directory to the *users* group. For logon scripts to run, you must be sure not to unshare the *NETLOGON* resource.

Note: Permissions automatically assigned for the directory identified by the `scripts` keyword affect only scripts stored in that directory. If you keep scripts in another directory, be sure to give the appropriate users R permission for these scripts.

For more information about permissions and the *users* group, see Chapter 3.

On an MS-DOS system, the filename extension for a batch file is *.bat*; on an MS OS/2 system, the extension is *.cmd*. If you use batch files as logon scripts on a network with both MS-DOS and MS OS/2 clients, keep identical copies of each script under two filenames, one with the *.bat* and one with the *.cmd* extension.

When you identify a batch file as a logon script while creating or modifying a user's account, type just the filename with no extension. When the user logs on, LAN Manager will add the appropriate extension automatically, depending on the operating system at the client. For example, identifying *clerk* as a user's script for a user causes *clerk.bat* to run when the user logs on at an MS-DOS client and *clerk.cmd* to run when the user logs on at an MS OS/2 client.

LAN Manager provides a simple logon script named *netlogon* (*.bat* and *.cmd*). This script simply displays the following message:

```
Welcome to LAN Manager 2.2.
```

The following sections describe how to use LAN Manager's Replicator service to maintain identical sets of logon scripts on each logon server in the domain and how to set up logon scripts for users of clients running earlier versions of LAN Manager.

Replicating Scripts

In a domain with backup domain controllers, a user's logon request is not necessarily processed by the same server each time the user logs on. If a logon script is run for the user, it is read from the server validating the logon request. For this reason, you must keep identical sets of logon scripts on the primary controller and each backup controller.

The Replicator service makes it easy to maintain identical sets of scripts on all logon servers in a domain. You add or change scripts on just one server (usually the primary domain controller), which is designated the export server. This server sends updates automatically to the other servers (usually the backup domain controllers), which are designated as import servers. You do not make changes directly to the scripts on the import servers.

Note: The following procedure applies to domains where only LAN Manager 2.0 or later is running. In domains with some clients running earlier versions of LAN Manager, see the procedure in the next section.

If you designate a primary and one or more backup domain controllers during installation, Steps 1 through 3 of the following procedure are performed automatically, and it is not necessary for you to repeat them. In this case, begin with Step 4 of the procedure.

Procedure. To set up the replication of logon scripts after installation with the primary domain controller as the export server, follow these steps:

1 On the primary domain controller, create a subdirectory named *scripts* under the directory *lanman/repl/export*.

2 Change the following keywords in the primary's *lanman.ini* file:

- In the *[netlogon]* section:

  Enter `scripts=repl/export/scripts.` If you change the value while the Netlogon service is running, you must stop and restart the Netlogon service for the change to take effect. For instructions on stopping and restarting the Netlogon service, see Chapter 7.

- In the *[replicator]* section:

  Check that `exportpath=repl/export.` This is the default value.

  Enter `replicate=export` or `replicate=both.` Change the value of `exportlist` to the name of the domain.

3 Change the following keywords in the *lanman.ini* file of each backup controller in the domain:

- In the *[netlogon]* section:

  Check that `scripts=repl/import/scripts`.

- In the *[replicator]* section:

  Check that `importpath=repl/import`.

  Enter `replicate=import` or `replicate=both`.

  Change the value of `importlist` to the servername of the primary domain controller.

4 Create logon scripts in the *lanman/repl/export/scripts* directory of the primary.

These scripts will be copied to the *lanman/repl/import/scripts* directory on each backup. Whenever you make changes to scripts on the primary, they are also copied to the backups, as long as the Replicator service is running.

This procedure uses default values for `exportpath`, `importpath`, and `scripts` to simplify the instructions for setting up the replication of scripts. Whether you use the default values or substitute other values, you must follow these rules for logon script replication to work:

- On each primary and backup server, keep the scripts in the directory identified by that server's `scripts` keyword or in a subdirectory of that directory.

- On the export server (usually the primary domain controller), the directory that contains the scripts must be a subdirectory of the directory identified by the `exportpath` keyword.
- On the import servers (usually the backup domain controllers), the directory that contains the scripts must be a subdirectory of the directory identified by the `importpath` keyword.
- In order for the files NETLOGON.BAT and NETLOGON.CMD to be replicated correctly, there must be some difference between the files internally. If you simply copy NETLOGON.CMD to NETLOGON.BAT, and make no changes to the directories, the checksum used during replication does not change, and the new filename is not copied. After you have copied one filename to another, make a minor change, such as adding a blank line, in one of the files so that they will be replicated correctly.

For more information about the Replicator service, see Chapter 7.

Scripts for Earlier Clients

A client running an earlier version of LAN Manager ignores the value of the `scripts` keyword in the *[netlogon]* section of the *lanman.ini* file on LAN Manager 2.0 or later servers. An earlier client expects to find the logon script identified for a user's account in the user directory (*/home/lanman* by default) specified by the `userpath` keyword in the *[server]* section of *lanman.ini*, or in a subdirectory of this directory. (LAN manager automatically creates a *scripts* subdirectory under */home/lanman* when a server is installed.)

If your domain has some clients running running versions earlier than 2.0 of LAN Manager, you have the following options for setting up scripts for users of the earlier clients:

- Use the procedure in the previous section to set up logon scripts.

  Users with LAN Manager 2.0 or later clients will use scripts in the primary domain controller's *lanman/repl/export/scripts* directory and in the backup domain controllers' *lanman/repl/import/scripts* directories.

  Set up scripts for users with earlier clients in the */home/lanman* directory or in a subdirectory of that directory on each logon server. These scripts will not be replicated.

- Enter `scripts=/home/lanman/scripts` in the *[netlogon]* section of the *lanman.ini* file on the primary and on each backup. All users who log on in the domain will use scripts in this directory.

  To replicate scripts from the primary to the backup controllers, set the following keywords in the *[replicator]* section of the *lanman.ini* file:

  — on the primary, `exportpath=/home/lanman`

  — on each backup, `importpath=/home/lanman`

  Note that when you do so, any other directories you want to replicate from the primary must also be subdirectories of */home/lanman*, because the Replicator service replicates only subdirectories of the single directory specified by the `exportpath` keyword.

Managing Groups

To make administration of user accounts easier, you can define groups of users and assign them groupnames. (Note that LAN Manager groups are not the same as UNIX system group IDs.) Groups simplify server administration, such as assignment of access permissions, when a number of users have similar needs on the LAN. To make a change that affects all users in a group, you do not have to list each of the group's members individually. In addition, when you add a new user account to a server and add that user to an existing group, the new user takes on the same permissions already assigned to the group.

A group can consist of any number of users, and each user can be a member of up to 253 groups: the 252 that you can define plus the *admins*, *users*, *guests*, and *servers* groups, whose memberships are mutually exclusive.

Note: Groups cannot be nested, that is, a group cannot be a member of another group.

Groups that you create on a domain's primary controller are copied automatically to the backup domain controllers and member servers, just as user accounts and security settings are.

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

- creating a new group
- changing a group's membership
- cloning a group
- deleting a group

Creating a Group

To create a group using the Net Admin Interface, follow these steps:

1. From the Accounts menu, select Groups.

   The Select a User Group dialog box appears.

2. Select the Add group command button.

   The Add a New User Group dialog box appears.

   The Non-members list box shows the names of all user accounts in the server's database.

3. In the Groupname text box, type a name for the new group.

   A groupname can be up to 20 characters long and can include letters, numbers, and the following characters: ! # $ % & ( ) - . @ ^ _ ` { } ~

4. In the Comment text box, optionally type a comment describing the group.

   This comment will be displayed when the list of groups on the server is viewed.

5 In the Non-members list box, move the highlight to the name of a user to be added to the new group, then select the Add member command button.

The selected username moves from Non-members to the Members list box.

6 Repeat Step 5 as many times as necessary to select all the members for the new group.

7 Select the OK command button.

The Select a User Group dialog box returns.

8 Windows — Select the OK command button.

MS OS/2 — Select the Done command button.

Equivalent net Command. You can also create a group using the **net group** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Changing a Group's Membership

You can add users to or remove users from a group at any time.

Note: You cannot use the following procedure to change the *admins*, *guests*, or *users* groups, whose memberships are determined by the privileges assigned to users.

To change the membership of a group using the Net Admin Interface, follow these steps:

1 From the Accounts menu, select Groups.

The Select a User Group dialog box appears.

2 In the list box of existing groups, move the highlight to the group whose membership you want to change, then select the `Zoom` command button.

The `View the User Group` dialog box appears.

3 To add a member to the group, in the `Non-members` list box, move the highlight to the name of a user to be added, then select the `Add member` command button.

The selected username moves from `Non-members` to the `Members` list box.

4 To remove a member from the group, in the `Members` list box, move the highlight to the name of a user to be removed, then select the `Remove` command button.

The selected username moves from `Members` to the `Non-members` list box.

5 Repeat Steps 3 and 4 as many times as necessary.

6 To remove all members from the group, select the `Remove all` command button.

7 Select the `OK` command button.

The `Select a User Group` dialog box returns.

8 Windows — Select the `OK` command button.

MS OS/2 — Select the `Done` command button.

Equivalent net Command. You can also add users to or remove users from a group using the **net group** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Cloning a Group

You can also create a new group by cloning, or using an existing group as a template for the new group. You can save effort by using this method, because the new group has all the same members and permissions as the original group. You can then change only those group attributes that you want to be different, such as by deleting and adding members and changing selected permissions. You can clone any group, including the special groups *users*, *admins*, and *guests*.

Note: You can clone a group only through the Net Admin Interface; there is no equivalent command-line command.

To clone a group using the Net Admin Interface, follow these steps:

1. From the `Accounts` menu, select `Groups.`

   The `Select a User Group` dialog box appears.

2. In the list box of existing groups, move the highlight to the name of the group to serve as the template, then select the `Clone` command button.

   The `Add a New User Group` dialog box appears. The `Members` list box shows the members of the template group.

3. In the `Groupname` text box, type a name for the new group.

4. In the `Comment` text box, optionally type a comment describing the group.

5. Adjust the group membership by adding or removing users as necessary, as described in the previous section, "Changing a Group's Membership."

6 Select the OK command button.

The Select a User Group dialog box returns.

7 Windows — Select the OK command button.

MS OS/2 — Select the Done command button.

Deleting a Group

Deleting a group removes the groupname from the user accounts database, together with all resource access permissions assigned to that group. The user accounts of the group's members are not affected, but it may change their ability to access resources.

Note: You cannot delete the special groups *users*, *admins*, *guests*, and *servers*.

To delete a group using the Net Admin Interface, follow these steps:

1 From the Accounts menu, select Groups.

The Select a User Group dialog box appears.

2 In the list box of existing groups, move the highlight to the name of the group to be deleted, then select the Delete command button.

A request for confirmation appears.

3 To confirm, select the OK command button.

The Select a User Group dialog box returns.

4 Windows — Select the OK command button.

MS OS/2 — Select the Done command button.

Equivalent net Command. You can also delete a group using the **net group** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Chapter 5

Managing Shared Directories

Overview

The Server Program lets you define access to the directories on each server's hard disk, including the root directory and any subdirectory or file. You can specify which directories are to be shared, which users and which groups are to have access to each shared directory, and what kind of access each user and group is to have.

This chapter describes how to manage access to a server's shared directories. It provides discussions of the following topics:

- viewing shared directories
- sharing directories on a server
- sharing directories from remote UNIX system clients/ servers through the NFS and RFS file systems
- unsharing directories
- setting permissions and auditing for a disk resource
- maintaining shared disks

For information about using shared disk resources, see either the *LAN Manager User's Guide for MS-DOS* or the *LAN Manager User's Guide for MS OS/2*.

Default Shared Resources

When you install the Server Program, LAN Manager provides the following default shared resources on the UNIX system:

ADMIN$ is the special administrative resource.

IPC$ supports interprocess communication.

C$ is the server's *root* (/) directory.

DOSUTIL contains MS-DOS programs and utilities for using and administering the LAN.

OS2UTIL contains MS OS/2 programs and utilities for using and administering the LAN.

PRINTLOG accumulates printer fault or error messages generated by the UNIX system.

LIB contains header files and link-time libraries needed to create LAN Manager applications.

USERS contains user home directories. This shared directory is created only when logon validation is enabled.

NETLOGON is the default location for logon scripts. This directory is shared if the Netlogon service is running.

REPL$ This directory is shared if the Replicator service is running.

Viewing Shared Directories

Viewing the directories shared by a server allows you to see which directories are available to the network. Before sharing a new directory from the server, first use the Net Admin Interface to check which directories (and sharenames) are currently shared.

To view the shared directories for your server using the Net Admin Interface, follow these steps:

1. From the `View` menu, select `Shared resources.`

   The `Shared resources` dialog box appears with a list box of shared directories on this server, showing the sharename, path, and a remark for each shared directory.

2. To show the special administrative resources *ADMIN$*, *IPC$*, *C$*, and (if the Replicator service is running) *REPL$*, mark the `Show hidden shares` check box.

3. To see more information about a shared directory, move the highlight to that directory's name in the list box and select the `Zoom` command button.

   The `Shared Resource Information` dialog box appears. In addition to the directory's sharename, path, and remark, this dialog box shows the maximum number of users that can use this directory and a list box of users currently using it.

4 Select the `Cancel` command button.

The `Shared resources` dialog box returns.

5 Windows — Select the `OK` command button.

MS OS/2 — Select the `Done` command button.

Equivalent net Command

You can also view shared directories using the **net view** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Using the UNIX System Administrative Interface to View Shared Directories

To view the shared directories on a server using the UNIX System Administrative Interface, follow these steps:

Caution Only *one* person should use the UNIX System Administrative Interface at any given time; otherwise, data may be lost.

1 Access the `LAN Manager Server` menu, as described in Chapter 2.

2 Select `Show shared directories.`

The system displays a list of the shared directories available to the network.

3 Press the CANCEL function key to return to the `LAN Manager Server` menu.

Sharing a Directory

By sharing a server's directories, you ensure that selected users on the LAN have access to the same copy of data files or programs in those directories. It also saves overall disk space by eliminating the need to keep duplicate copies of files on clients.

In order for a client to link to a shared directory, the client must be running the same protocol stack as the server.

Note: Remember that the software license for an application program must allow access by multiple users if you are going to share it on the server.

Sharing directories also makes it possible for users to archive files on a server's hard disk rather than on diskettes. Hard-disk storage is generally more reliable than diskette storage.

Since many users will depend on shared directories, it is recommended that you periodically back up the server's hard disk. For instructions, see the section "Backing Up and Restoring Server Files" later in this chapter.

When the Server Program is started, it establishes default UNIX system directories on the server as the location for creating new shared directories. When you create a new shared directory, you must specify its location on the server. If you supply the name of a directory that does not already exist, the Server

Program will attempt to create it. It is recommended that you put new shared directories under one of the default administrable directories, such as */home* or */home2*. If you try to share a directory in some other location on the server, and that directory does not already exist, whether the directory is created depends upon the UNIX system permissions of the parent directory.

When you share directories on a server's hard disk, it is important for the disk to be well-organized. If a number of users access the same directory for different purposes and activities, the directory will soon be a clutter of unrelated files. If you take the time to create and share separate directories organized by group and function, it will be easier to keep files organized.

Although it might seem easiest to share an entire hard disk with all users on the LAN (by specifying the disk's *root* directory), organizational and security problems are likely to result.

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

The default directories are created in the following file systems:

- */home/lanman*
- any non-Remote File Sharing (RFS) file system mounted at a mount point named */homeN/lanman*, where *N* is a number from 2 to 9

Using the UNIX System Administrative Interface, you can create new directories or mount new file systems on the server (for example, */home2*) where the UNIX system will allow creation of new shared directories.

To share a directory on a server running user-level security, you must share the directory and then set permissions to give groups and users access. When you share a directory, you can also set up the auditing of certain types of access and the auditing of specific files and subdirectories. The following sections describe how to perform all of these tasks.

When you share a directory on a server running share-level security, all subdirectories and files under the shared directory assume the permissions of the parent directory. Since auditing is either enabled or disabled under share-level security, you do not specify auditing for each resource.

Before performing the following procedure, you should have prepared a list of all directories you need to share on the server. You also need a list of users and groups that will have access to each shared directory and the kinds of permissions they require. For information about disk access permissions, see Chapter 3.

Procedure. To share a directory using the Net Admin Interface, follow these steps:

1 From the `View` menu, select `Shared resources.`

  The `Shared Resources` dialog box appears.

2 Select the `Add share` command button.

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

3 Select the Disk directory option button.

4 Select the OK command button.

The Share a Directory with the Network dialog box appears.

5 In the Sharename text box, type a sharename for the directory.

A sharename must follow MS-DOS file naming conventions. The sharename does not have to be the same as the directory name.

The following words must not be used as sharenames; net use commands to shares with any of these names will fail: COMM, DEV, MAILSLOT, PIPE, PRINT, QUEUES, SEM, and SHAREMEM.

If the directory does not exist, LAN Manager prompts you to confirm that you want it to create the directory.

6 Do *one* of the following:

- Using the Path text box: type the complete path (including the drive ID, **c:**) of the directory that you want to share.
- Using the Contents of text box:

  a Windows — Select the Directory command button.

  MS OS/2 — Select the Dir command button.

  A list box of directories appears.

  b To select a directory and see a list box with its contents, move the highlight to the name of the directory and select the Dir command button again.

As you move the highlight, the text in the `Contents of` text box changes to show the selected directory.

- **c** To return to the directory one level up, with `..` (parent directory) highlighted in the text box, select the `Dir` command button.
- **d** Repeat Steps b and c until the `Contents of` text box contains the name of the directory you want to share.

7 In the `Remark` text box, optionally type a comment describing the shared directory. When users view a list of available resources, they will see this comment.

8 To specify the number of users allowed to access the directory at one time, from the `User limit` option buttons, select *one* of the following:

- `Unlimited` to set no limit.
- `Max users` to set a limit.

  If you select this button, in the adjacent text box, type the maximum number of users allowed. If a number appears in this text box when you select the button, the value is from the `maxclients` keyword in the *[server]* section of the server's *lanman.ini* file. You can type over it with a lower number, but you cannot exceed it.

9 To restrict the directory to users with admin privilege, mark the `Admin only` check box.

10 Select the `OK` command button.

If the server is running user-level security, you are prompted for access permissions.

11 Do *one* of the following:

- To specify permissions and audited events for the directory or its subdirectories and files now, go to Step 2 of the procedure in the section, "Setting Permissions and Auditing for a Disk Resource."
- To end this procedure, follow these steps:

  For Windows clients:

  a Select the `Done` command button.

  The `Shared Resources` dialog box returns.

  b Select the `OK` command button.

  For MS OS/2 clients:

  a Select the `Done` command button.

  The `Share a Directory with the Network` dialog box returns.

  b Select the `Cancel` command button.

  The `Shared Resources` dialog box returns.

  c Select the `Done` command button.

Equivalent net Command. You can also share a directory using the **net share** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Sharing Remote Directories Using NFS and RFS

UNIX system computers that are running the Server Program can mount remote directories on other UNIX system computers using either NFS or RFS. These remote directories can then be shared through the Server Program, like any local UNIX system directory, to LAN Manager users.

Note: RFS is not supported on the NCR® UNIX system.

To share directories, you must do the following:

1 Start either NFS or RFS, then do one of the following:

- If you wish to use NFS, start NFS on both your local server and your remote UNIX system computer. For additional information, refer to the *UNIX SVR4 Network User's and Administrator's Guide.*
- If you wish to use RFS, start RFS on both your local server and your remote UNIX system computer. For additional information, refer to the *NCR System 3000 Network File System.*

2 Share a directory on the remote computer through either NFS or RFS.

- If you wish to share a directory through NFS on AT&T® UNIX system and NCR computers, use the following command.

  ```
  share -F nfs -o rw,soft unixsharepath
  ```

  where *unixsharepath* is the full path of the directory you wish to share (for example */home2/dir1*).

  For additional information on sharing, refer to either the *UNIX SVR4 Network User's and Administrator's Guide* or the *NCR System 3000 Network File System.*

- If you wish to share a directory through RFS on AT&T UNIX system computers, use the following command.

  ```
  share -F rfs -o rw -d "description" unixsharepath resource
  ```

  where *"description"* is an optional remark describing the shared directory, *unixsharepath* is the full UNIX system path of the directory to be shared, and *resource* is the RFS sharename to be used by the computers that will mount the directory.

  For additiional information on sharing, refer to the *UNIX SVR4 Network User's and Administrator's Guide.*

3 Make the appropriate additions and/or changes to the NFS and RFS setups. Refer to the next section "Setup Consideratons" for detailed information.

4 Mount the remote directory on the local computer that is running the LAN Manager 2.2 server.

- If you wish to mount a directory through NFS on AT&T UNIX system or NCR computers, use the following command:

  ```
  mount -F nfs -o rw,soft unixname:unixsharepath mountpoint
  ```

  where *unixname* is the name of the remote UNIX system computer (without the **.serve** extension) whose directory you wish to mount, *unixsharepath* is the full UNIX system path of the remote directory, and *mountpoint* is the full local UNIX system path to where you wish to place the remote directory on your local server.

  For additional information, refer to either the *UNIX SVR4 Network User's and Administrator's Guide* or the *NCR System 3000 Network File System.*

- If you wish to mount a directory through RFS on the AT&T UNIX system, use the following command:

  ```
  mount -F rfs -o rw resource mountpoint
  ```

  where *resource* is the RFS sharename given to the remote directory when it was shared on the remote computer and *mountpoint* is the full local UNIX sytem path where you wish to place the remote directory on your local server.

  For additional information on mounting, refer to the *UNIX SVR4 Network User's and Administrator's Guide.*

5 Use the procedure in the section "Sharing a Directory" earlier in this chapter to share the remote directory or subdirectory to LAN Manager users through the Server Program.

Setup

Before you can share directories, you must check your NFS and RFS setups. Review and make the appropriate changes with regard to the following setup considerations for NFS and RFS.

NFS Setup Considerations

- The remote directory that you wish to share should have the UNIX system permission `777`.
- The remote directory that you wish to share must be shared with the NFS permission RW.
- You do not need the parameter `root=` when sharing through NFS.

RFS Setup Considerations

- The remote directory that you wish to share should have the UNIX system permission `777`
- The remote directory that you wish to share must be shared with the RFS permission RW.
- On the remote UNIX system computer, you must map users and groups across the RFS share using the following procedure.

Procedure. To map the users and groups, follow these steps:

1. Log on as **`root`**.
2. Start the UNIX System Admin Interface as described in Chapter 2.
3. Select `network_services` by using the arrow keys, then press ↵.

   The `Network Services Management` menu appears.
4. Select `remote_files` by using the arrow keys, then press ↵.

   The `Distributed File System Management` menu appears.
5. Select `specific_ops` by using the arrow keys, then press ↵.

   The `Other Distributed File System Operations` menu appears.
6. Select `rfs` by using the arrow keys, then press ↵.

   The `Other Remote File Sharing Operations` menu appears.
7. Select `id_mappings` by using the arrow keys, then press ↵.

   The `User and Group ID Mapping Management` menu appears
8. Select `set uid mapping` by using the arrow keys, then press ↵.

9. Select `0to99guest`, then press SAVE.

   The system returns you to the id_mappings menu.

10. Select `set gid mappings` by using the arrow keys, then press ↵.

11. Select `0to9guest`, then press SAVE.

12. Press EXIT to exit.

Setting Permissions and Auditing for a Disk Resource

When you share resources under user-level security, you should assign access permissions for each resource. You may need to review the assigned permissions under the following circumstances:

- when users cannot access resources they need
- when unauthorized users are accessing a resource

Under user-level security, LAN Manager maintains a database of access permissions for disk resources, regardless of whether those resources are currently shared. Therefore, if you stop sharing a resource and then later share it again, LAN Manager remembers the access permissions you assigned previously for the resource. Every resource starts with default permissions; if you change them, they remain as changed until you change them again.

You must assign permissions for each drive or directory, or else accept the default access permissions.

You may need to change access permissions under the following circumstances:

- when you want to stop using the default permissions for a resource
- when you want to assign, change, or delete permissions for a user or group

Some programs, such as Microsoft Word for Windows, maintain temporary files by renaming the source file to a temporary name, and then, when the user saves the file creates a new file with the name of the source file. The temporary file is then deleted. The permissions that have been assigned to a specific file are not assigned to the new file that has the same filename; they apply only to original file, which has been renamed (to the temporary filename) and then deleted. The updated file is treated as a completely new file by LAN Manager, which means it inherits the permissions of the directory in which it resides. Files that are likely to go through this kind of updating process should be kept in directories that have the permissions you want these files to inherit.

Note: When you share a file resource, the `File Permissions` dialog box will appear automatically to allow you to assign permissions on that resource.

Procedure. To assign permissions using the Net Admin interface for Microsoft Windows, follow these steps:

1 From the Accounts menu, choose **File Permissions**. The `File Permissions` dialog box appears.

2 Select or type in the file or directory for which you want to view or set permissions.

3 After the appropriate share, file, or directory is selected and is listed in the

    "Setting permissions for"
    box in the
    middle of the screen, use the two list boxes at the
    screen to assign permissions to users.

    Usernames and groupnames are found in the users with

and users without permissions. Groups are denoted
of the name.

4 Above the

Users with permissions list box, there is a row of small buttons. Similar buttons appear beside each name in the list box. The letters on these buttons refer to the permissions that can be assigned:

R	Read
W	Write
C	Create
X	Execute
D	Delete
A	Change attributes
P	Set permissions

Procedure. To assign permissions for a username or groupname, follow these steps:

1. If the username or groupname appears in the Users with permissions list box, assign permissions on the selected resource by selecting the name and choosing the small buttons that correspond to the permissions you want to grant.
2. Highlight the name and choose the appropriate permission buttons above the Users with permissions list box.
3. Highlight the name and press Alt + the appropriate permission letter. For example, pressing Alt + X grants execute permission on the selected resource to the highlighted username.

   The letters for assigned permissions will be highlighted on the line with the username or groupname; and when that line is highlighted, the corresponding letters will also be highlighted in the row of buttons above the list box.

Procedure. To remove a permission for a username or groupname, follow these steps:

Choose the button with the letter from the line with the username. The button will no longer be highlighted.

Procedure. To remove all permissions for a username or groupname, follow these steps:

Select the name and choose **Revoke**.

The name will be transferred to the `Users without permissions` list box.

Procedure. To revoke all permissions for all names, follow these steps:

Choose **Revoke all**.

If the username or groupname to which you want to assign permissions appears in the `Users without permissions` list box, you must transfer it to the `Users with permissions` box in order to assign permissions. To do so, simply highlight the name and choose **Permit**. When you choose **Permit**, any permissions that are highlighted in the buttons at the top of the `Users with permissions` box will be assigned to the username being transferred. You can, of course, alter these permissions later by selecting the username or groupname, and choosing the appropriate buttons in the `Users with permissions` list box. The permissions assigned to the last username or groupname highlighted in the `Users with permissions` box remain highlighted when you select a name in the `Users without permissions` box, allowing you to easily duplicate assigned permissions.

You can also select permissions from the buttons above the `Users with permissions` box after you select the name to transfer but before you choose **Permit**.

Because the permissions buttons remain highlighted after you transfer the username or groupname, you can easily assign identical permissions to several users. To transfer all names from the `Users without permissions` list box to the `Users with permissions` list box, granting them the selected permissions, choose **Permit all**. You can make further adjustments to permissions in the `Users with permissions` list box.

Note: Only 64 unique usernames are supported. By assigning individual users to groups, you can simplify the task of assigning permissions, and keep within the 64-name limit.

If you choose **Permit tree** from the `File Permissions` dialog box, you will be prompted for confirmation for each change.

Procedure. To set auditing for the directory or file, follow these steps:

1 Select the `Audit` command button.

The `Auditing the Resource` dialog box appears.

2 To turn on auditing and specify audited events, follow these steps:

a Mark the `Auditing enabled` check box.

b Do *one* of the following:

- To designate the events to be audited, mark the appropriate `Audited events` check boxes.
- To audit all of the listed events, select the `Set all` command button.

c Select the `OK` command button.

The `Access Permissions` dialog box returns.

3 Select the `OK` command button.

The `Select a File for Access Permissions` dialog box returns.

4 If, in the previous steps, you specified permissions and auditing for a directory, and if you want them to apply to all subdirectories and files under that directory, select the `Permit tree` command button.

Note: If you are using the Net Admin Interface for Windows, you will be prompted for verification for each file being changed. You can stop the process at any point by choosing **Cancel**. Permissions that have been set up to that point will remain in effect.

If you are using the Net Admin Interface for MS OS/2 clients or the command line, the process cannot be canceled after it begins. In addition, the process can be lengthy, depending on the number of files involved.

5 To specify permissions and audited events for additional directories and files, repeat Steps 2 through 8 as many times as necessary.

6 Select the `Done` command button.

Equivalent net Command. You can also provide access and set permissions and auditing for a shared directory or file using the **net access** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*. For more information about auditing resources and the audit trail, see Chapter 7.

Changing Permissions as a Non-Administrative User

When you assign P access permission to a user, you allow that user to change access permissions on a resource. This is very different from assigning administrative privilege. A user with admin privilege can change access permissions on any resource, while a user with P access permission can change access permissions only on the specific resource for which that permission is assigned.

Typically, P access permission is assigned to a non-administrative user only when the shared resource is the user's own home directory. If you assign a non-administrative user P access permission for a shared resource, be sure to explain the meaning of that permission to the user. For more information on P access permission, see Chapter 3.

Unsharing a Directory

You may need to stop sharing a directory when the 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 using the Net Admin Interface, follow these steps:

1. From the `View` menu, select `Shared resources.`

   The `Shared Resources` dialog box appears.

2. In the list box of shared resources, move the highlight to the name of the directory that you want to unshare, then select the `Stop sharing` command button.

   A request for confirmation appears.

3. Windows — Select the `Yes` command button to confirm.

   MS OS/2 — Select the `OK` command button to confirm.

4. Windows — Select the `OK` command button.

   MS OS/2 — Select the `Done` command button.

Equivalent net Command. You can also stop sharing a directory using the **net share** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Maintaining Shared Disks

Because a number of users may be able to create files in a shared directory, the hard disk on a server is likely to fill up much more quickly than on a client. As administrator, you should closely monitor the amount of disk space being used. The Server Program provides an automatic warning when a server's disk is nearly full. To conserve disk space, encourage users to take inventory of their files from time to time and to delete files they no longer need.

It is important to back up all shared directories regularly. You should have a backup copy for each server hard disk in case of disk failure. It is also recommended that you save archive copies of files you no longer want on the hard disk before you delete them.

Managing Server Disk Space

To ensure efficient use of network resources, you should regularly check the amount of server disk space available. If there is too little free disk space, you will need to make more available.

Caution Do not use the *root* directory (/) to store files and directories created by the server. If you do, you may exhaust free disk space in the root file system and cause the server's UNIX system to crash.

The UNIX system provides commands that allow you to evaluate per-user and total disk usage on the server. These commands are summarized below. For complete information about these commands, see the documentation provided with the UNIX operating system.

To check disk space usage by a single user, at the UNIX system prompt, type **`du -s`** *user* and press ↵. Replace *user* with the complete path to the user's login directory, starting at *root* (/).

The system displays the number of data blocks occupied by the named user.

To determine total disk space usage on the system, type **`df -v`**, then press ↵.

The result is a display similar to the following:

```
File      Free      Total     Percent
System    Blocks    Blocks    Full
------    ------    ------    -------

/         3072      20088     84%
/home     48918     149364    67%
/home2    64432     114210    43%
```

You can also use the **chkstor** command on the server to check disk usage. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Backing Up and Restoring Server Files

To back up and restore server files, you can use either of the following methods:

- Use the MS-DOS **xcopy** command or the **backup** and **restore** commands, as described in your MS-DOS user's guide.
- Use the UNIX System Administrative Interface as described in your UNIX system administrator's guide.

Using the UNIX System Administrative Interface, you can quickly back up all relevant files on your server. Using the **xcopy** command, you must back up one shared directory at a time.

In addition to user files and network applications, you should back up all files in the *lanman* and */home/lanman* or */home2/lanman* directories. These files contain information on the server's shared resources (disk and non-disk resources and home directories). If these files are corrupted or lost and no backup is available, you will have to repeat the entire setup process to recreate them.

Chapter 6

Managing Shared Printers

Overview

As an administrator, you must decide which printers to share with network users and how to share them. When sharing printers, you must set up printer queues and decide whether to create pools of printers.

In addition to printers connected to the server, you can share client printers, which are printers connected to specially configured MS-DOS clients. Although shared client printers can be physically connected only to MS-DOS clients, they can be accessed by any client on the network.

This chapter provides information on the following topics:

- configuring a port for a printer connected to the server
- setting up a shared client printer
- shared printer queue operation
- sharing a printer queue
- defining a printer reset sequence
- unsharing a printer queue
- managing shared printer queues and print jobs

Configuring a Port for a Printer Connected to the Server

After you have connected a printer to your server, you must configure the printer port. (To connect and configure the printer itself, see the instructions included with the printer.) Use the procedure in this section to configure the server's printer ports for printers that are physically connected to the server. (Additional information about configuring the printer port appears in your UNIX System administrator's guide.)

The same steps are used for both serial and parallel printer ports. This procedure uses a parallel port as an example.

Note: Before using this procedure, you must know the printer type, that is, the generic name for the printer. Typically, the printer type is the manufacturer or model name, for example, hplaserjet.

Before you configure a postscript printer that is directly connected to the internal serial port on the server, you must check to see if any process is running on the port. If a process is running, refer to the *LAN Manager Troubleshooting and Command Reference*.

If you have already configured the server's printer ports for connected printers, go on to the section "Understanding Shared Printer Queues" later in this chapter.

To configure a printer port for a printer connected to the server, you must use the UNIX System Administrative Interface, following these steps:

Caution Only *one* person should use the UNIX System Administrative Interface at any given time; otherwise, data may be lost.

1 At the server console, log in as `root`.

2 At the # prompt, type **`sysadm printers`** and press ↵.

   If the system prompts you for the **sysadm** password, type the password.

   The `Line Printer Services Configuration and Operation` menu appears.

3 Select `printers`.

   The `Configure Printers for the Printer Service` menu appears.

4 Select `add`.

   The `Add a New Printer` form appears.

Note: To help you configure the printer port as quickly as possible, the following steps direct you to accept defaults when possible. You can press the HELP function key for information on acceptable responses to any prompt or acceptable values for any field.

5 In the `Printer name:` field, type a name for the printer you are adding, consisting of up to 14 lowercase letters and numbers only, and press ↵.

6 In the `System name:` field, the system supplies the server's UNIX system name. Press ↵.

7 In the `Printer type:` field, do one of the following:

- Use the CHOICES function key to select a printer type and then press ↵.
- If the printer type is post or pt, type **ps** in the `Printer type:` field, then press ↵.

8 In the `Similar printer to use for defaults:` field, use the CHOICES function key to make your selection and then press ↵.

9 In the `Do you want to use standard configurations? (eg, alerts, banners):` field, press ↵ to accept the default, `yes`.

Note: If you are configuring a port for a PostScript® printer, use the CHOICES function key to change the response to `no` and then press ↵.

10 In the `Do you want to use standard port settings? (eg, baud rate, parity):` field, press ↵ to accept the default, `yes`.

11 In the `Device or Basic Networking address:` field, use the CHOICES function key to select an address and then press ↵.

12 When the form is complete, press the SAVE function key.

13 Do *one* of the following:

- If you selected standard configurations (answered `yes`) in Step 9, a confirmation that the printer has been added is displayed. Go on to Step 14.
- If you did not select standard configurations (answered `no`) in Step 9, the `Configure New Local Printer` form appears. Use the CHOICES function key to select values for each of the fields on this form.

  Note: If you are configuring a port for a PostScript printer, in the `File types printable without filtering` field, type **`postscript`**

  When the form is complete, press the SAVE function key.

  A confirmation that the printer has been added is displayed.

14 Press the [CONT] function key.

Several different forms may appear. If you did not select the standard configuration, the `Setup Printer Access` form will appear. Depending on the printer type, the `Software Selectable Character Set Aliasing for Printer` form may appear.

15 Do *one* of the following:

- If the `Setup Printer Access` form appears, follow these steps:

  a Use the [CHOICES] function key to select values for each of the fields complete the form.

  b When the form is complete, press the [SAVE] function key and go to Step 17.

- If the `Software Selectable Character Set` form appears, follow these steps:

  a Press the [SAVE] function key.

  The `Setup Printer Access` form appears.

  b Use the [CHOICES] function key to select values for each of the fields and complete the form.

  c When the form is complete, press the [SAVE] function key and go on to Step 17.

- If neither the `Setup Printer Access` form nor the `Software Selectable Character Set` form appear, go on to Step 16.

16 Do *one* of the following:

- If you selected standard port settings (answered `yes`) in Step 10, the `Configure Printers for the Printer Service` form returns. Go on to Step 17.
- If you did not select standard port settings (answered `no`) in Step 10, the `Printer Communication Setup Subtask` form appears. Use the [CHOICES] function key to select values for each of the fields in this form.

  Note: If you are configuring a port for a PostScript printer, select `none` in the `parity` field. You must also set your printer for no parity. Refer to your printer manual for more information.

  When the form is complete, press the [SAVE] function key.

17 Press the [CANCEL] function key.

The `Line Printer Services Configuration and Operation` menu returns.

18 Press the [EXIT] function key.

19 To confirm that the printer is set up correctly, follow these steps:

a At the UNIX system shell prompt, type the following, replacing *printername* with the printer's name, to allow the printer to accept jobs:

```
usr/sbin/accept printername
```

Then press ↵.

b At the UNIX system shell prompt, type the following to enable the printer:

```
/usr/bin/enable printername
```

Then press ↵.

c At the UNIX system shell prompt, type the following:
`lp -d`*`printername`* `/etc/passwd`.
Press ↵.

The system displays the following messsage:
`request id is` *printername* -# (1 file)

d Do *one* of the following:

- If the printer prints out the */etc/passwd* file (a list of UNIX system logins on your server), it is functioning properly.
- 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. Next, check the printer cable installation. Finally, check the printer configuration information. Then repeat Step a.

  For additional troubleshooting information, see your UNIX system administrator's guide.

You have completed configuring the server's printer port for this printer; users logged on to the server can now use it. However, to allow network users to use this printer, you must now create a shared printer queue, as described later in this chapter in the section "Sharing a Printer Queue."

Setting Up a Shared Client Printer

The Server Program provides access not only to printers connected to the server, but also to printers connected to Basic MS-DOS and Enhanced MS-DOS clients. These printers are called shared client printers.

Once designated as a shared printer, a client printer can print jobs sent by users from any kind of client. This feature provides additional flexibility in configuring the LAN, allowing you to put shared printers close to users. It also increases the number of available shared printers independent of the number of printer ports available on the server.

Note: Client printing requires the use of extra network resources. If it is difficult to connect the client to which the printer is attached to the usual number of network resources, you may need to make sure enough resources are allocated in your transport protocol to support the establishment and disconnection of virtual circuits to your shared client printers.

In addition, if you will be printing large graphics files at this printer, you may need to increase the value of the maximum file size kernel parameters, `HFSZLIM` and `SFSZLIM`, in the UNIX system on the server. For information on tuning kernel parameters, refer to your UNIX system administrator's guide.

To make a client printer available to LAN users, you must first use the UNIX System Administrative Interface (sysadm) to configure the server to recognize the printer. Then you must load the LAN Manager spooler agent software on the client to which the printer is connected.

Three sets of spooler agent software are supported by LAN Manager:

- the LAN Manager **clispool** command that works with the MS-DOS **print** command
- the LAN Manager **clipcach** command that works with the LaserTools PrintCache™ program, Version 2.4a or later, consisting of the LaserTools **pcache** and **print** commands

- the LAN Manager Print Station utility that allows you to share a printer that is connected to an MS-DOS client without the intervention of a server.

Clispool and Print Commands. The Clispool Program is an MS-DOS terminate-and-stay-resident (TSR) program kept in the server's *DOSUTIL* shared directory. The Clispool Program receives print jobs from the server and sends them to the MS-DOS **print TSR** program for printing. To receive print jobs from a server, the Clispool Program automatically links to the server's spool directory associated with that client printer (*lanman/clipr/printername*).

The *print.com* file is an MS-DOS TSR program that enables MS-DOS users to print files in the background while using other commands or applications. For information about the **print** command, see your MS-DOS manual.

Note: If the **clispool** and **print** commands will be used to print jobs at a shared client printer, the MS-DOS *print.com* file must be on the hard disk of the client to which the printer is connected.

Clipcach Command and PrintCache Program. The *clipcach.exe* file is an MS-DOS TSR program kept in the server's *DOSUTIL* shared directory. The Clipcach Program receives print jobs from the server and sends them to the LaserTools **print TSR** program command, which in turn sends the jobs to the **pcache** program for spooling and printing. To receive print jobs from a server, the Clipcach Program automatically links to the server's spool directory.

LaserTools *print.com* is an MS-DOS TSR program that provides the **clipcach** command and the user with an interface similar to the MS-DOS **print** command. PrintCache is a LaserTools TSR program that provides for spooling and printing files in the background while a user is using other commands or applications. For information about the LaserTools **pcache** and **print** commands, see your LaserTools PrintCache manual.

Note: If you are using a PostScript printer, you must use the **clipcach** command and PrintCache program. You must also set the printer for no parity. Refer to your printer manual for more information.

When the LAN Manager Print Station utility is started on a workstation, the workstation appears as a server to the network. This allows other users to connect to the printer, as they would to any other network printer. However, only the Print Station owner can view and control the print queue on that Print Station.

In the default implementation of LAN Manager Print Station, print jobs are written to a file on the *host* computer (the one running **printsta**), and then sent to the printer. This process, called spooling, allows the person sending the print job to regain control of his or her computer without waiting for the job to print. If the disk space for temporary print files is not available, you can load LAN Manager Print Station with spooling disabled.

Printing takes place as a background task on the host computer; the person using that workstation will not be interrupted by print jobs from other users.

The **netpopup** utility will send messages to the host workstation when the LAN Manager Print Station encounters errors such as "printer out of paper."

If you load LAN Manager Print Station in non-spooling mode, or if print jobs will be spooled from workstations running MS OS/2, you should not have messsages sent to the host workstation. Disable the **netpopup** utility.

For information on setting up and using the LAN Manager Print Station Utility, refer to the *LAN Manager User's Guide for MS-DOS*.

Procedure. To configure a client printer for **clispool** or **clipcach** only, you must use the UNIX System Administrative Interface, following these steps:

Caution Only *one* person should use the UNIX System Administrative Interface at any given time; otherwise, data may be lost.

1 Access the `LAN Manager Server` menu, as described in Chapter 2.

2 Select `Printer Administration`.

The `Printer Administration` menu appears.

3 Select `Define Client Printers`.

A list box of currently configured client printers, if any, appears. Go on to Step 4, 5, or 6, as appropriate.

4 To add a client printer, follow these steps:

a Press the ADD function key.

The `Add a Client Printer` form appears.

b In the `Client computername:` field, enter the name of the client (up to 14 lowercase characters) to which the shared printer is to be connected, and press ↵.

c In the `Printer type:` field, use the CHOICES function key to select from a list of supported printers. When your selection is highlighted, press ↵.

Note: If your printer is not listed, select a listed printer that is compatible. See your printer manual for more information about emulations supported by your printer.

d Press the SAVE function key.

The system displays progress messages while adding the printer, ending with a confirmation message.

e Press ↵ to continue.

The `Add a Client Printer` menu returns.

f If necessary, repeat Steps b through e for as many client printers as you need to configure.

g Press the CANCEL function key.

An updated menu of installed printers appears.

5 To change a client printer, follow these steps:

a Move the highlight to the name of the appropriate printer, then press the CHANGE function key.

The Change Printer form appears.

b In the Printer type: field, press the CHOICES function key for a list of supported printers. Move the highlight to the name of the appropriate printer, then press ↵.

Note: If your printer is not listed, select a listed printer that is compatible. See your printer manual for more information about emulations supported by your printer.

c Press the SAVE function key.

The system displays progress messages while changing the printer configuration, ending with a confirmation message.

d Press ↵ to continue.

The Change Printer form returns.

e Press the CANCEL function key.

An updated menu of installed printers appears.

6 To delete a client printer, follow these steps:

a Move the highlight to the name of the appropriate printer, then press the DELETE function key.

The system displays a warning that Delete will remove the selected client print device and prompts you for confirmation.

b To confirm, type `y` and press ↵.

The system displays a confirmation that the selected printer has been deleted.

c Press ↵ to continue.

An updated menu of installed printers appears.

7 Do *one* of the following:

- To add, change, or delete additional client printers, repeat Step 4, 5, or 6, as appropriate.
- If you have finished configuring all client printers, the next step is to add the printer to a shared printer queue. Skip to the sections "Understanding Shared Printer Queues" and "Sharing a Printer Queue" later in this chapter. After adding the printer to the queue, return to this step of this procedure.

8 Perform this step and the next at the MS-DOS client to which the printer is connected.

Do *one* of the following:

- If you are using the LAN Manager **clispool** command and the MS-DOS **print** command as your spooler agent software, edit the client's *autoexec.bat* file to add the following lines:
  - — If the printer is a serial printer, at any point after the `net start workstation` line, add the line

    ```
    mode comn:9600,n,8,1,P
    ```

    Replace *n* with the serial port number.

Refer to your MS-DOS manual for additional information on the **dos mode** command.

- Immediately after this `mode` command line (for a serial printer) or at any point after the `attstart` line (for a parallel printer), add the line

  ```
  print /d:portid
  ```

  Replace *portid* with the ID of the port on the client to which the printer is connected (for example, **LPT1** or **COM1**).

- Immediately after this `print` line, add the line

  ```
  clispool /i /s:driveid
  ```

  Replace *driveid* with an unused drive letter, within the allowable range, that the Clispool Program will use to link to its spool directory on the server. Do not type a colon (:) after the drive letter.

  For more information on the **clispool** command, see either the *LAN Manager User's Guide for MS-DOS* or the *LAN Manager User's Guide for MS OS/2*.

- If you are using the LAN Manager **clipcach** command and the LaserTools PrintCache program as your spooler agent software, edit the client's *autoexec.bat* file to add the following lines:

Caution

If the MS-DOS **print** command is on the hard disk, it must be deleted or renamed to prevent conflicts with the LaserTools **print** command. In addition, the LaserTools PrintCache program must be installed on the hard disk of the client to which the printer is connected. Be sure that the directory containing the PrintCache program is included in the path of the client to which the printer is connected.

— At any point after the `net start workstation` line, add the line

```
pcache
```

— Immediately after this `pcache` line, add the line

```
print /d:portid
```

Replace *portid* with the ID of the port on the client to which the printer is connected (for example, **LPT1** or **COM1**).

— Immediately after this `print` line, add the line

```
clipcach /i /s:driveid
```

Replace *driveid* with an unused drive letter that the Clipach Program will use to link to its spool directory on the server. Do not type a colon (:) after the drive letter.

For more information on the **clipcach** command, see either the *LAN Manager User's Guide for MS-DOS* or the *LAN Manager User's Guide for MS OS/2*. For more information on the **pcache** and **print** commands, see your LaserTools PrintCache manual.

9 Execute the modified *autoexec.bat* file, either by rebooting the client or by typing `autoexec` and pressing ↵.

10 To check that the printer is functioning as a shared printer, follow these steps at *another* client:

   a At the client's system prompt, link to the printer by typing

   ```
   net use portid: \\uname.serve\queue name
   ```

   and pressing ↵.

   Replace *portid* with an unused port ID on the client, *uname* with the server's UNIX system name, and *queuename* with the name of the shared printer queue.

   b Print the second client's *config.sys* file by typing

   ```
   copy config.sys portid:
   ```

   and pressing ↵.

   Replace *portid* with the same port ID used in Step a.

If the client printer is functioning properly as a shared printer, it will print the *config.sys* file.

Note: If the client printer is not the only printer associated with the shared printer queue, the file will print out at the first available printer in the queue.

Understanding Shared Printer Queues

A shared printer is a printer that can be accessed by LAN users with the appropriate permissions. A shared printer can be connected directly to the server (via serial or parallel port) or to a Basic MS-DOS or Enhanced MS-DOS client on the LAN. The server's *lp* system (providing UNIX system information for handling print jobs) mediates between the Server Program and the printer, so that print jobs can execute while users perform other tasks at their clients.

Users access shared printers by sending their print jobs over the network to the shared printer queues that you create. A single shared printer queue may consist of many shared printers, or it may contain programs called print processor scripts that process print jobs and send them to a shared printer or other destination. A shared printer queue is accessed over the network like any other shared resource.

Printer Queue Operation

When a user sends a print job to a shared printer queue, the job can be routed to its final destination in one of the following ways:

- The shared printer queue sends the print job directly to the server's *lp* subsystem, which forwards the job to the printer(s) in the printer queue.

- The shared printer queue sends the print job to a print processor script. As administrator, you program the print processor script, and therefore define its function.

  The print processor script may send the print job to the server's *lp* subsystem, which will forward it to the printer(s) in the printer queue, or it may send the job to some other destination, such as another UNIX system.

The Server Program automatically sends a message to the user to notify him or her when and where the job is printed. The Server Program also notifies users if there are problems with print jobs (if the printer is capable of such notification) or changes in the status of print jobs (for example, if an administrator pauses the queue).

The Server Program allows you to create simple shared printer queues that send print jobs to one printer and more sophisticated shared printer queues that send print jobs to a pool of printers. When setting up a shared printer queue, you must consider these options:

- which printers should receive print jobs from this queue
- what priority level you want to assign to this queue
- at what times the shared print queue service should print jobs
- whether you want to use a print processor script to process jobs sent to this queue
- whether you want to use a printer-specific reset sequence (set through the UNIX System Administrative Interface) to process print jobs sent to this queue

- whether you want a separator page to be printed between print jobs for this queue and, if so, what that page will look like

The following sections describe these options and how they are associated with shared printer queues.

Printer Queue Configurations

There are a number of ways you can configure printer queues. In order of increasing complexity, you can configure:

- a single shared printer queue associated with a single printer
- a single shared printer queue associated with multiple printers of the same type, connected to any servers and/or clients in the LAN
- multiple shared printer queues (each with different options) associated with one or more printers

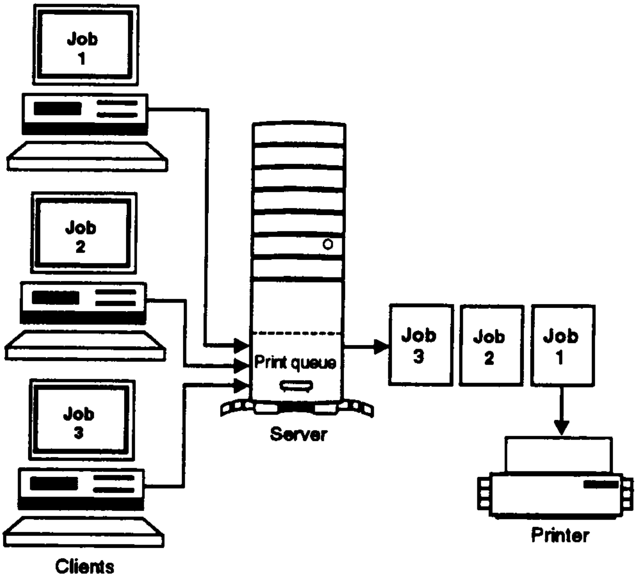
Single Queue Associated with a Single Printer

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 printer queue and the printer's devicename on the server.

Note: Printer devicenames must conform to the naming conventions of the UNIX operating system: a devicename can be up to 14 characters long and can include only letter, numbers, and the underscore (_) character.

Figure 6-1 illustrates a single queue, single printer configuration. In this configuration, as the queue receives multiple print jobs, it sends the first job to the printer and stores the remaining jobs until the first job has finished printing.

Figure 6-1: Single Shared Printer Queue, Single Printer



Single Queue Associated with Multiple Printers

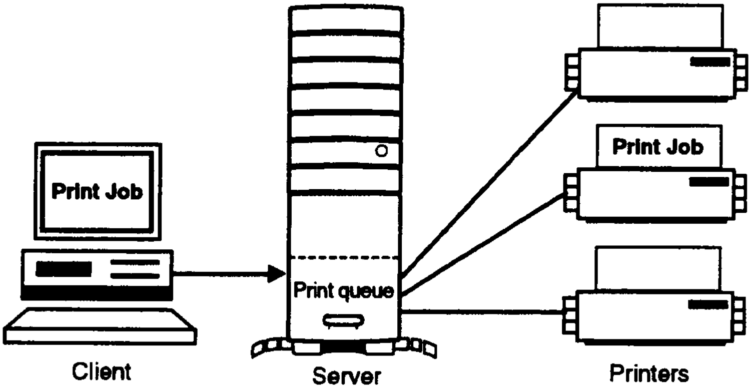
When you assign two or more printers of the same kind to a single shared printer queue, you are creating a pool of printers. A single queue routed to a pool of printers is convenient for users. The Server Program searches for an available printer, and automatically routes a print job to the first available printer in the pool of printers associated with the queue. This is an efficient way to share a group of similar printers.

The Alerter service (described in Chapter 7) sends the user a message to inform him or her which printer has printed the job.

To create a shared printer queue associated with two or more printers, you must define a sharename for the queue and devicenames for all printers in the pool.

Figure 6-2 illustrates a single queue, multiple printer configuration.

Figure 6-2: Single Shared Printer Queue, Multiple Local Printers



A printer queue can route jobs to printers on more than one server. The remote printers are shared in a single queue on the local server, and connections are made from the local server to the remote servers. You create the printer queue on the local server, specifying the computernames of the remote servers and the devicenames of the local printers.

You can also make a printer connected to a client available to as many users as the printer queue is configured to allow.

For instructions on using remote printers, see the section "Setting Up a Shared Client Printer" in this chapter.

Figures 6-3 and 6-4 illustrate configurations in which a single queue accesses both local and remote printers.

Figure 6-3: Single Shared Printer Queue, Local and Remote Printers

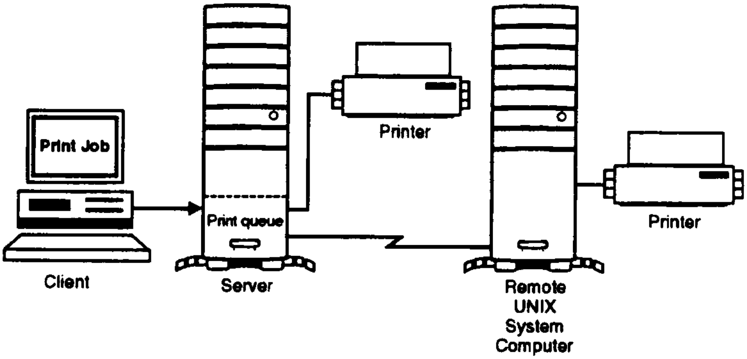
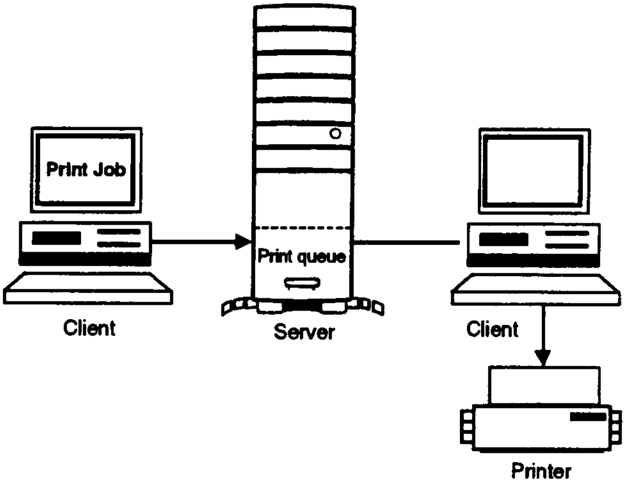


Figure 6-4: Single Shared Printer Queue, Local and Remote Printers



Multiple Queues Associated with One or More Printers

You can assign two or more shared printer queues to the same printer or group of printers. This approach is especially useful if you configure the queues differently. For example, you can assign different access permissions for each queue to different groups and users, different priority levels to different queues, and different times at which the queues can send jobs to the printers.

You can also use this method if you have an application that requires a special print processor. You would create one queue using that processor to handle all jobs from that application and another queue to handle all other print jobs.

Figure 6-5 illustrates a multiple queue, single printer configuration.

Figure 6-5: Multiple Shared Printer Queues, Single Printer

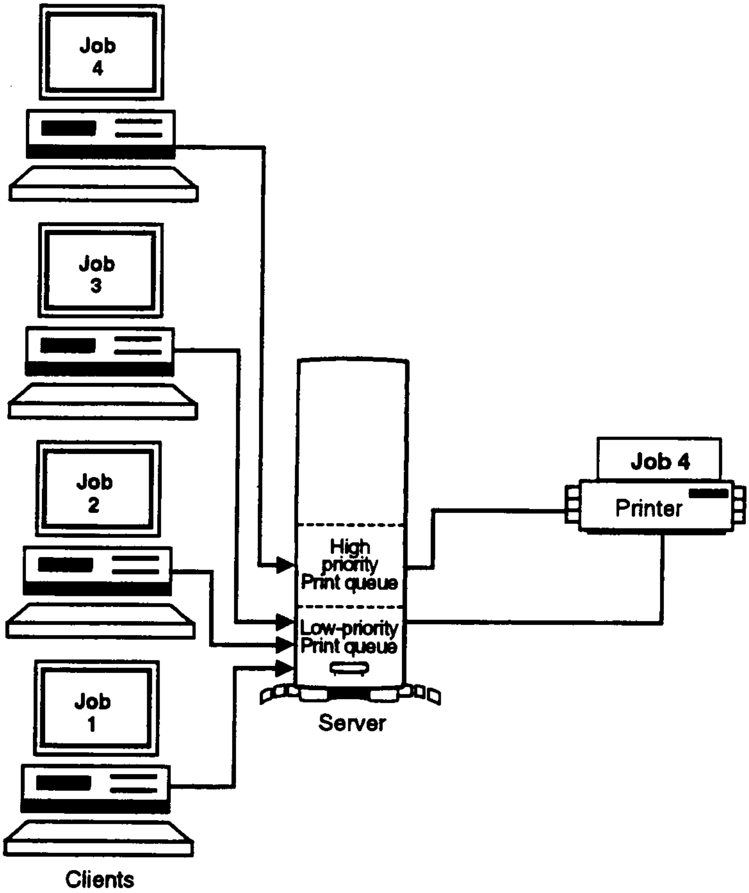
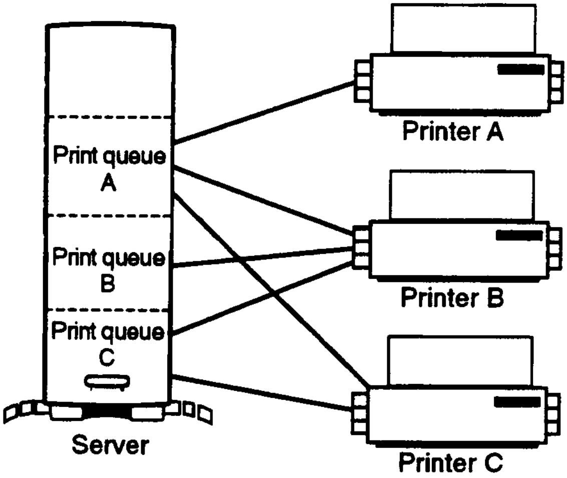


Figure 6-6 illustrates a more complex configuration, with multiple queues accessing multiple printers. In this configuration, Queue A sends jobs to Printers A, B, and C; Queue B sends jobs only to Printer B; and Queue C sends jobs to Printers B and C. This configuration offers flexibility and convenience both to the administrator who needs to set up different queues for different purposes and to users who need a queue that routes jobs to the next available printer.

Figure 6-6: Multiple Shared Printer Queues, Multiple Printers



Printer Queue Options

The option settings for a printer queue control the configuration of the queue — how the queue accesses printers and uses a print processor and separator page. This section describes each option. For information about how to set these options, see the section "Setting and Changing Options" later in this chapter.

Priority

As an administrator, you can assign a shared printer queue a priority level ranging from 1 (highest) to 9 (lowest). The default priority level is 5. If certain kinds of print jobs are more time-critical than others, you can create two queues with different priority levels for the same printer or printer pool, and assign access to the higher-priority queue only to users producing critical jobs.

Scheduling

The scheduling option lets you specify the times at which a shared printer queue can send print jobs to the printers. Users can submit print jobs at any time, but the queue holds all requests until the designated time.

Print Processor Scripts

You can use the print processor option to specify the filename of a print processor script for the shared printer queue. A print processor script is a program for manipulating print jobs. Instead of sending a print job directly to the server's *lp* subsystem, the queue sends it to the designated script for processing. The script can send its output into a pipe to the *lp* subsystem or another destination, such as a file or a terminal.

A print processor script must be an executable UNIX system file. You can create a script using a text editor or the UNIX System Administrative Interface. For more information, see the section "Creating a Print Processor Script" later in this chapter.

Printer Reset Sequences

The Server Program lets you define reset sequences for a shared printer queue so that print jobs sent to printers in the queue can use special printing functions available on those printers. For example, you can use reset sequences to print jobs in landscape mode instead of portrait mode, or in a different typeface than the default.

For more information about printer reset sequences, see the section "Defining a Printer Reset Sequence" later in this chapter.

Parameters

The Server Program supports the following parameters for shared printer queues. (The valid values for each parameter are listed in the section "Setting and Changing Options" later in this chapter.)

`COPIES`	specifies how many copies of a print job should be printed.
`TYPES`	specifies the content type (or file type) of the files that will be sent to the printer queue.
`EJECT`	specifies whether or not a page feed is required between copies for a multiple-copy print job.
`BANNER`	specifies whether or not a separator page (or banner) is required between print jobs.

Separator Page

The Server Program automatically prints a separator page, or banner, before each print job. You can alter the default banner and create one more suitable to your needs. When you share a printer queue and set queue options, as described in the section "Setting and Changing Options" later in this chapter, you can specify the name of an ASCII text file containing your banner page.

Printer Queue Security

As an administrator, you control user access to shared printer queues in one of the following ways:

- On a server running share-level security, you can assign a password to a printer queue, and only users who know the password can access the queue. You can also share a queue as admin only, which makes it available only to a user who has made a connection to the *ADMIN$* resource. (A user who needs to print graphics from Presentation Manager applications must also connect to the server's *IPC$* resource.)
- On a server running user-level security, you can assign permissions to users and groups. There are three levels of permissions for printer queues on servers running user-level security:

Y (yes)	The user can send jobs to the queue.
N (no)	The user cannot send jobs to the queue.
Y+P (yes + change permissions)	The user can send jobs to and set access permissions for the queue.

If several printer queues will be serving the same or similar groups of users, it may be useful to create a default set of printer queue permissions. You can assign these defaults quickly to a new queue simply by marking the `Use default permissions` check box when you share the queue. For instructions, see the next section.

Sharing a Printer Queue

Note: Before you can create and share a printer queue on the server, the UNIX system must be configured for each printer associated with the queue. For instructions, see the section "Configuring a Port for a Printer Connected to the Server" or the section "Setting Up a Shared Client Printer" earlier in this chapter.

In order for a client to link to a shared printer, the client must be running the same protocol stack as the server.

To share a printer queue using the Net Admin Interface, follow these steps:

1 From the `View` menu, select `Shared resources.`

The `Shared Resources` dialog box appears.

2 Select the `Add share` command button.

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

3 Select the `Printer` option button, then select the `OK` command button.

The `Share a Printer Queue with the Network` dialog box appears, with a list box of printer queues that are created but are not currently shared, if any. If the server is running share-level security, the `Password` text box also appears in the dialog box.

4 Do *one* of the following:

- To share an existing queue, in the `Queue` list box, move the highlight to an existing queuename.
- To create a new shared queue, in the `Sharename` text box, type a new sharename of up to 12 characters.

  Note: A sharename can only include letters, numbers, and the (_) character.

5 In the `Remark` text box, optionally type a comment describing the printer queue.

Users viewing the resources available on the server will see this comment.

6 *On a server running share-level security only*:

In the `Password` text box, type a password of up to 15 characters.

7 To specify the number of users allowed to access the queue at one time, from the `User limit` option buttons, select *one* of the following:

- `Unlimited` to set no limit.
- `Max users` to set a limit.

  If you select this button, in the adjacent text box, type the maximum number of users allowed. If a number appears in this text box when you select the button, the value is from the `maxclients` keyword in the *[server]* section of the server's *lanman.ini* file. You can type over it with a lower number, but you cannot exceed it. (For information on raising the value of maxclients, see Chapter 7.)

8 To make the queue accessible only to administrators, mark the Admin only check box.

9 Select the OK command button.

If a printer queue with the sharename you entered does not already exist, LAN Manager prompts you to confirm that you want to create it. (Note that you cannot use the same sharename for more than one queue.)

10 On Windows clients, select the Yes command button to confirm.

On MS OS/2 clients, select the OK command button to confirm.

The Printing Options for Queue dialog box appears. For instructions on setting options, see the section "Setting and Changing Options" later in this chapter.

11 Select the OK command button.

The Add Permissions for Printer Queue dialog box appears. If the server is running user-level security, go on to the section "Setting Permissions and Auditing for Printer Queues " and Named Pipes" later in this chapter.

Equivalent net Command. You can also share a printer queue using the **net share** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Using the UNIX System Administrative Interface to Share a Printer Queue

To create and share a printer queue using the UNIX System Administrative Interface, follow these steps:

Caution Only *one* person should use the UNIX System Administrative Interface at any given time; otherwise, data may be lost.

1 Access the `LAN Manager Server` menu, as described in Chapter 2.

2 Select `Printer Administration.`

The `Printer Administration` menu appears.

3 Select `Administer Printer Queues.`

A menu of existing shared printer queues (if any) appears.

4 Press the SHARE function key.

The `Share a New Printer Queue` form appears.

5 In the `Queue name:` field, type a unique sharename for the queue. A queuename can be up to eight characters long and can include letters, numbers, and the (_) character.

You cannot use a name that is already assigned to one of the UNIX system *lp* devices on the server, or a name already assigned to a shared resource on the server. (By pressing the CHOICES function key, you can display the names of existing unshared printer queues. You can use one of these, or type a new name.)

6. In the `Processor script:` field, use the [CHOICES] function key to select from the existing print processor scripts. When the name of the script you want to use appears in the field, press ↵.

   If you do not plan to use a print processor script, select `None`.

7. In the `Print device(s):` field, press the [CHOICES] function key to display a list of configured printer devicenames. Move the cursor to the name of a printer to be included in this queue and press the [MARK] function key. Repeat this step for as many printers as you want to include in the queue.

   Note: If you are using a print processor script, you can leave this field blank.

8. Press the [SAVE] function key to save your selections.

   Your selections appear in the `Print device(s):` field.

9. Press the [CANCEL] function key to continue.

10. When the form is complete, press the [SAVE] function key.

    The system displays progress messages while adding the printer queue, ending with a confirmation message.

11. Press ↵ to continue.

    The `Share a New Printer Queue` form returns.

12 Press the CANCEL function key.

The updated menu of shared printer queues appears.

13 Press the CANCEL function key again.

The `Printer Administration` menu returns.

If the server is running user-level security, the *users* and *guests* groups automatically have access permissions for the new shared printer queue.

Note: If ASCII files will be sent to this queue for printing on PostScript printers, you must define the content type (or file type) of the files that will be sent to the queue as **`simple`**, as follows:

- If you are performing remote administration, at the client's system prompt, type the following line and press ↵:

```
net admin \\uname.serve /c net print sharename
/parms:types=simple
```

where *uname* is the name of the server and *sharename* is the name of the printer you are sharing.

- If you are working at the server console, at the system prompt, type the following line and press ↵:

```
net print sharename /parms:types=simple
```

where *sharename* is the name of the printer you are sharing.

For more information on the **net print** command, see the *LAN Manager Troubleshooting and Command Reference*.

Setting and Changing Options

To set and/or change options on printer queues, you must use the Command Line Net Interface. Refer to the following to set and/or change options:

- To set/change priority use, type
  `net print /priority:number`

- To set/change print device use, type
  `net print /route:`*devicename*
- To set/change more than one print device, separate each devicename with a comma.
- To set/change separator file use, type
  `net print /separator:`*pathname*

  You can supply a relative or absolute pathname. Relative pathnames are assumed to begin in the server's *lanman/spool* directory; absolute pathnames begin at the root (/) directory.
- To set/change the time you wish a job to begin printing, type
  `net print /after:`*time*
- To set/change the time you wish printing to stop, type `net print /until:`*time*
- To set/change a print processor script, type
  `net print /processor:`*pathname*

  A full pathname is not required. Since all print processor script files are kept in the server's *lanman/customs* directory; no other location is allowed.
- To set/change printer queue parameters, use the `net print /parms:`*parm=value* `command`, with the following options for *parm*:

`COPIES`	Specifies how many copies of a print job should be printed. Type a number greater than zero. The default is 1.
`TYPES`	Specifies the default content type (or file type) of the files that will be sent to the printer queue. The content type accepted by a queue is determined by the content type accepted by the first

Note: You will not need to change the automatically assigned TYPES value unless you are sending ASCII files to a queue that includes PostScript printers. For a queue including PostScript printers, enter TYPES=simple. If you do not, the print jobs will fail, but the queue will return the normal confirmation message.

For more information about content types, see the section on configuring printers in your UNIX system administrator's guide.

EJECT Specifies whether a page feed is required between copies for a multiple-copy print job. Specify auto (the default) or yes if you want page feeds between copies. Specify no if you do not.

BANNER Specifies whether or not a separator page (or banner) is required between print jobs. Specify yes or no.

For example, to specify two copies separated by a page feed and a separator page, type

```
net print /PARMS:COPIES=2
EJECT=yes BANNER=yes
```

Setting Permissions and Auditing for Printer Queues and Named Pipes

On a server running user-level security, you can set access permissions and audited events when you share a printer queue. You can also change the values you have set previously for a queue. You may need to do so under the following circumstances:

- when you want to stop using default permissions for the queue
- when you want to assign, change, or delete permissions for a group or user
- when you want to turn auditing on or off

Note: Use the following procedure to set permissions and auditing for named pipes as well.

Procedure. To set permissions and auditing for a shared printer queue or named pipe using the Net Admin Interface, follow these steps:

1 Do *one* of the following:

- For a new shared printer queue, follow the procedure in the "Setting and Changing Options" section earlier in this chapter.
- For an existing queue or pipe, follow these steps:

  a From the `Accounts` menu, select `Other permissions.`

  The `Select a Queue or Pipe for Access Permissions` dialog box appears.

  b From the `Access type` option buttons, select `Print queues` or `Named pipes.`

c In the Resource name list box, do *one* of the following to select a queue or pipe:

- — To set default permissions and auditing, mark Default, then select the Zoom command button.

  Default permissions are assigned for a queue or pipe for which you do not set permissions and auditing individually.

- — To set permissions and auditing for a queue or pipe that does not appear in the list box, select the Add entry command button.

- — To change the permissions and auditing for a queue or pipe, move the highlight to its sharename, then select the Zoom command button.

2 The View Permissions or Add Permissions dialog box appears, with the following list boxes:

- Permitted shows groups and users with permissions to access the queue or pipe. Groupnames are marked with an asterisk (*).
- Not permitted shows all other groups and users.

3 To assign permissions for the queue or pipe, do *one or more* of the following, as appropriate:

- To assign default permissions to all printer queues, see the next section, "Setting Default Permissions."

- To assign permissions to a group or user, in the `Not permitted` list box, move the highlight to the groupname or username; from the `Assigned permission` option buttons, select the permission you want to assign; then select the `Permit` command button.

  The groupname or username moves to the `Permitted` list box.

- To change the permissions for a group or user, in the `Permitted` list box, move the highlight to the groupname or username. In the `Assigned permissions` check boxes, mark the appropriate permissions.

  The permissions displayed in the `Permitted` list box change as you mark and unmark check boxes.

  Note: If the permission option button is set to `No` when you move a user into the `Permitted` list box, you are preventing that user from accessing the queue or pipe, regardless of the permissions assigned to the groups to which that user belongs.

- To revoke the permissions for a group or user, in the `Permitted` list box, move the highlight to the groupname or username, and select the `Revoke` command button.
- To revoke permissions for all users, select the `Revoke all` command button.

- If you are setting permissions for an actual queue or pipe, to assign the default permissions, mark the `Use default permissions` check box.

4 To audit successful or denied attempts to use this resource (or both), mark one or both `Enable auditing for` check boxes.

5 Select the `OK` command button.

The `Select a Queue or Pipe for Access Permissions` dialog box returns.

6 Select the `Done` command button.

Equivalent net Commands. You can also set permissions and auditing for a shared printer queue or named pipe using the **net share, net print**, and **net access** commands. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Setting Default Permissions

By default, no permissions are granted on named pipes or printer queues. However, you can set custom defaults for each of these types of resources by assigning permissions to the `* (Default)` resource for that resource type. This "resource" does not point to an actual queue or named pipe and you will not see it listed when you view shared resources. This "resource" exists only to allow you to set custom defaults for the resource type. You can then assign these custom defaults to any resource of that type by checking the `Use default permissions` box in the View Permissions for ... dialog box. If you neither assign specific permission nor check the `Use default permissions` box, no permissions will be set for that resource.

Procedure for Enhanced MS-DOS with Windows Clients. To assign permissions to `* (Default)`, follow these steps:

1 From the `Accounts` menu, select `Other permissions`.

  The `Other Permissions` dialog box appears.

2 From the `Available/Shared Resources` list box, select the type of resource for which you want to set custom defaults.

3 From the `Setting permissions` for: dialog box, select `* (Default)`.

4 Select the `SAVE` command button.

5 Select the `Done` command button.

Procedure for MS OS/2 Clients. To assign permissions to `* (Default)`, follow these steps:

1 From the Accounts menu, select `Other permissions`.

  The `Select a Queue or Pipe for Access Permissions` dialog box appears.

2 From the `Access type` list box, select the type of resource for which you want to set custom defaults.

3 From the `Resource` name list box, select `* (Default)`.

4 Select the `ZOOM` command button.

  `The View Permissions for` ... dialog box appears.

5 Assign permissions. Do not check `Use default permissions` when setting permissions for `* (Default)`.

6 Select the `OK` command button.

The `Select a Queue or Pipe for Access Permissions` dialog box appears.

7 Select the `Done` command button.

Creating a Print Processor Script

By default, the Server Program sends all print jobs to the *LP* subsystem of the UNIX system, which queues and prints them using the **lp** command. However, the Server Program also allows you to create customized print processor scripts. A print processor script can send print jobs directly to a file or terminal instead of a printer, or to a remote UNIX system computer via the **uucp** command, or to another UNIX system process, such as **troff** or **nroff**.

When you create a print processor script, you must share a queue that uses it to allow users to access it. You can share a queue using the Net Admin Interface or the UNIX System Administrative Interface. (For instructions, see the appropriate section earlier in this chapter.) To access the script, users link to the queue, and then use a print command such as the MS-DOS **copy** command. You can define an unlimited number of print processor scripts for different purposes.

After you have created a print processor script, provide users with instructions on how to use it.

A print processor script is a UNIX system executable file. It should conform to the following guidelines:

- To avoid affecting service to other users, execute scripts in the background.
- Have your scripts make and operate on a temporary copy of the file to be printed, rather than on the original file. For example, make a line similar to the following the first line of any print processor script:

```
    cp $FILENAME /tmp/myfile$$
```

You can assign the following environment variables in a print processor script:

`$CLIENT`
is the name of the computer from which the print job was sent.

`$COPIES`
is the number of copies to be printed (1 and up).

`$PRIO`
is the UNIX system *LP* priority of the print job (1 to 39).

`$DEST`
is the UNIX system *LP* printer class (server queue) to which the job was sent.

`$FILENAME`
is the full pathname of the file to be processed.

Following is a sample print processor script that sends a file to a user named *john* on a remote system named *frodo*:

```
/bin/cp $FILENAME /tmp/myfile$$
(
/usr/bin/uuto /tmp/myfile$$ frodo!john
/bin/rm /tmp/myfile$$
) &
```

Using a Text Editor

To create a print processor script using a text editor, follow these steps:

1 Use a text editor (such as **vi**) to create a shell script.

2 Make the script executable by typing **chmod +x** *filename* and pressing ↵. Replace *filename* with the name of the script.

3 After you have tested the script and are satisfied that it works as intended, save it in the server's *lanman/customs* directory.

4 Share the printer queue that will use the script, using the procedure in the section "Sharing a Printer Queue" earlier in this chapter. When you fill out the `Printing Options for Queue` dialog box in that procedure, type the script's filename in the `Print processor` text box. If your print processor script requires arguments, you can append them after the name of the script.

Using the UNIX System Administrative Interface

To create, change, or delete a print processor script using the UNIX System Administrative Interface, follow these steps:

Caution Only *one* person should use the UNIX System Administrative Interface at any given time; otherwise, data may be lost.

1 Access the `LAN Manager Server` menu, as described in Chapter 2.

2 Select `Printer Administration.`

The `Printer Administration` menu appears.

3 Select `Edit Processor Scripts.`

If there are existing scripts on the server, the `Scripts` menu appears with a list of scripts. Go on to Step 4, 5, or 6, as appropriate.

If there are no existing scripts, the system prompts you to press the [ADD] function key to create a new script. Go on to Step 4.

4 To create a print processor script, follow these steps:

a Press the [ADD] function key.

The `Add a Script` form appears.

b In the `Script name:` field, type a unique name of up to 14 alphanumeric characters, then press the [SAVE] function key.

The system responds with a screen of instructions.

c Read the instructions, then press ↵ to continue.

The system prompts you to confirm that you want to create a processor script.

d To confirm, type `y` and press ↵.

The system displays more instructions, including a sample script and a list of the environmental variables that are available, and then prompts you to enter your script.

e Type your print processor script in its entirety. To end your input, type a line consisting only of a period (`.`).

The system displays the script as entered and prompts you to confirm that you want to save it.

f Do *one* of the following:

- To save the script, type `y` and press ↵.

  A confirmation message appears.

- To re-enter the script, type `n` and press ↵.

  The system prompts you again to enter your script. Return to Step e.

- To abort the procedure, type `q` and press ↵.

g Press ↵ to return to the `Scripts` menu.

5 To change a print processor script, follow these steps:

a Move the cursor to the name of the script you want to change.

b Press the CHANGE function key.

The system displays the contents of the script and prompts you to confirm that you want to change it.

c To confirm, type **y** and press ↵.

d Type the new version of the script in its entirety. To end your input, type a line consisting only of a period (.).

The system displays the script as entered and prompts you to confirm that you want to save it.

e Do *one* of the following:

- To save the script, type **y** and press ↵.

  A confirmation message appears.

- To re-enter the script, type **n** and press ↵.

  The system prompts you again to enter your script. Return to Step d.

- To abort the procedure, type **q** and press ↵.

f Press ↵ to return to the `Scripts` menu.

6 To delete a print processor script, follow these steps:

a Move the cursor to the name of the script you want to delete.

b Press the DELETE function key.

The system prompts you for confirmation.

c To confirm, type `y` and press ↵.

A confirmation message appears.

d Press ↵ to return to the `Scripts` menu.

7 Share the printer queue that will use the script, using the procedure in the section "Sharing a Printer Queue" earlier in this chapter. When you fill out the `Printing Options for Queue` dialog box in that procedure, type the script's filename in the `Print processor` text box.

Defining a Printer Reset Sequence

The Server Program allows you to define reset sequences for shared printer queues. Print jobs sent to a queue can use special printing functions available on the printers associated with the queue. For example, you can use reset sequences to print jobs in landscape mode instead of portrait mode, or in a different typeface than the default.

Because different printers use different reset sequences, all of the printers in a shared print queue must be of the same make and model for a reset sequence to work properly. You can define sequences either to precede (*preset* sequences) or to follow (*postset* sequences) print jobs for any shared printer queue. Typically, the preset sequence invokes a special function, and the postset sequence returns the printer to its default mode.

If a printer is associated with multiple shared printer queues, you can define a different sequence for each queue. For example, you might configure the queues so that a user can print a job in elite pitch by linking to *sharename1* or in pica pitch by linking to *sharename2*, even though both print jobs are printed on the same printer.

While you can define only one reset sequence per shared printer queue, the sequence can invoke more than one function. For example, the same sequence could specify both pica pitch and bold typeface.

You must enter reset sequences as hexadecimal characters. See your printer manual for the specific hexadecimal codes for your printer.

Procedure. You can define, change, or delete a reset sequence only through the UNIX System Administrative Interface. To do so, follow these steps:

Caution Only *one* person should use the UNIX System Administrative Interface at any given time; otherwise, data may be lost.

1 Access the `LAN Manager Server` menu, as described in Chapter 2.

2 Select `Printer Administration.`

The `Printer Administration` menu appears.

3 Select `Administer Printer Queues.`

A menu appears, listing the names of all shared printer queues, and showing for each queue its printer device names and whether or not it has a reset sequence.

4 Move the highlight to the desired queuename, then press the [PRE/POST] function key.

The `Printer Sequences` form appears.

Go on to Step 5, 6, or 7, as appropriate.

5 To define a new reset sequence, follow these steps:

a In the `Preset sequence:` field, type the hexadecimal codes for the preset print modes, separated by spaces.

   b. In the `Postset sequence:` field, type the hexadecimal codes for the postset print modes.

6. To change an existing sequence, follow these steps:

   a. In the `Preset sequence:` field, type over the existing sequence with the hexadecimal codes for the new preset sequence. If there are unwanted characters remaining, use the spacebar to delete them.

   b. In the `Postset sequence:` field, type over the existing sequence with the hexadecimal codes for the new postset sequence.

7. To delete an existing sequence, in the `Preset sequence:` and `Postset sequence:` fields, use the spacebar to delete all characters.

8. Press the **SAVE** function key.

   The system displays progress messages while changing the printer configuration, ending with a confirmation message.

9. Press ↵ to continue.

10. Press ↵ again to return to the `Printer Sequences` form.

11. Press the **CANCEL** function key.

    The `Administer Printer Queues` menu returns, showing any changes you made.

12. To define, modify, or delete a printer reset sequence for another queue, return to Step 4 and repeat the appropriate process.

Unsharing a Printer Queue

You may need to stop sharing a shared printer queue under any of the following circumstances:

- to reorganize shared printer queues
- to remove a printer (which affects the shared queue only if this printer is the only printer in the queue)
- when a particular shared printer queue has become unnecessary

To unshare a shared printer queue using the Net Admin Interface, follow these steps:

1. From the `View` menu, select `Shared resources.`

   The `Shared Resources` dialog box appears, with a list box of shared resources.

2. Move the highlight to the name of the queue you want to unshare, then select the `Stop sharing` command button.

   A request for confirmation appears.

3. On Windows clients, select the `Yes` command button to confirm.

   On MS OS/2 clients, select the `OK` command button to confirm.

4. On Windows clients, select the `OK` command button.

   On MS OS/2 clients, select the `Done` command button.

The queue still exists, and can be displayed using the **net print** command, but it is unavailable to network users.

Equivalent net Command. You can also unshare a printer queue using the **net share** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Using the UNIX System Administrative Interface to Unshare a Printer Queue

To unshare a shared printer queue using the UNIX System Administrative Interface, follow these steps:

Caution Only *one* person should use the UNIX System Administrative Interface at any given time; otherwise, data may be lost.

1 Access the `LAN Manager Server` menu, as described in Chapter 2.

2 Select `Printer Administration.`

The `Printer Administration` menu appears.

3 Select `Administer Printer Queues.`

A menu of shared printer queues appears.

4 Move the cursor to the name of the queue you want to unshare, then press the UNSHARE function key.

A request for confirmation appears.

5 To confirm, type **y** and press ↵.

A confirmation message appears.

6 Press ↵ to continue.

An updated menu of shared printer queues appears.

The queue still exists, but is unavailable to network users.

Managing Shared Printer Queues and Print Jobs

This section provides information on the following topics:

- viewing queues and job information
- holding and releasing a printer queue
- purging print jobs from a printer queue
- holding and releasing a print job
- restarting a print job
- moving a print job in a printer queue
- deleting a print job
- canceling a print job that is printing
- pausing and continuing a printer

Viewing Queues and Job Information

You can view a list box of the server's printer queues, a single queue, and the print jobs in each queue.

To view information about all the printer queues on a server using the Net Admin Interface, follow these steps:

1 From the `View` menu, select `Printer queues.`

The `Print Queues` dialog box appears, with a list box of queue names on the server, whether or not they are currently shared. Under the name of each queue is a list of the print jobs in that queue.

2 To see the options set for an individual queue, move the highlight to the queue name and select the `Zoom` command button.

The `Printing Options for Queue` dialog box appears, showing the options currently set for the selected queue.

3 On Windows clients, select the `OK` command button.

On MS OS/2 clients, select the `Cancel` command button.

The `Print Queues` dialog box returns.

4 On Windows clients, select the `OK` command button.

On MS OS/2 clients, select the `Done` command button.

To view information about a single printer queue on a server using the Net Admin Interface, follow these steps:

1 From the `View` menu, select `Shared resources.`

The `Shared Resources` dialog box appears.

2 In the list box of resources, move the highlight to the name of the queue you want to view and select the `View queue contents` command button.

The `Print Queue` dialog box appears, showing the queue name and status of the queue and a list box of the print jobs currently in the queue.

3 To view an individual print job, move the highlight to the job and select the `Zoom` command button.

4 On Windows clients, select the `OK` command button.

On MS OS/2 clients, select the `Done` command button twice.

Equivalent net Command. You can also view information about printer queues using the **net print** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Holding and Releasing a Printer Queue

You can hold a printer queue, preventing it from sending any jobs to printers. When you do so, the printers associated with the queue finish printing their current jobs, but all further jobs stay in the queue until the queue is released. Releasing the queue returns it to normal status.

Note: You cannot hold a queue that uses a print processor script. Even if you change the queue's status, it will continue to process and send print jobs.

Releasing a queue that is in an error condition will clear the error.

To hold or release a printer queue using the Net Admin Interface, follow these steps:

1 From the `View` menu, select `Printer queues.`

The `Print Queues` dialog box appears.

2 To hold a queue, in the list box of queues, move the highlight to the name of the queue you want to hold, then select the `Hold` command button.

The status message for the queue changes to

`Queue Held.`

3 To release a held queue, in the list box of queues, move the highlight to the name of the queue you want to release, then select the `Release` command button.

The status message for the queue changes to `Queue Active.`

4 On Windows clients, select the `OK` command button.

On MS OS/2 clients, select the `Done` command button.

Equivalent net Command. You can also hold or release a printer queue using the **net print** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Purging Print Jobs from a Printer Queue

You can purge a shared printer queue, that is, delete all jobs in the queue except the one currently printing.

To purge a printer queue using the Net Admin Interface, follow these steps:

1 From the `View` menu, select `Printer queues.`

The `Print Queues` dialog box appears.

2 In the list box of queues, move the highlight to the name of the queue you want to purge, then select the `Purge` command button.

A request for confirmation appears.

3 To confirm, select the `OK` command button.

4 On Windows clients, select the `OK` command button.

On MS OS/2 clients, select the `Done` command button.

Equivalent net Command. You can also purge a printer queue using the **net print** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Holding and Releasing a Print Job

As administrator, you can hold any print job that the queue has not yet sent to the printer. The held job stays in the queue until you release it; other jobs in the queue will be printed. Non-administrative users can hold and release their own print jobs.

To hold or release a print job using the Net Admin Interface, follow these steps:

1 From the `View` menu, select `Printer queues.`

The `Print Queues` dialog box appears.

2 To hold a job, in the list box of printer queues and print jobs, move the highlight to the job you want to hold, then select the `Hold` command button.

The status of the job changes to `Held.` The user who sent the job is notified that it is on hold.

3 To release a held job, in the list box, move the highlight to the job you want to hold, then select the `Release` command button.

The status of the job changes to `Waiting` or `Printing.` The user who sent the job is notified that it has been released.

4 On Windows clients, select the `OK` command button.

On MS OS/2 clients, select the `Done` command button.

Equivalent net Command. You can also hold or release a print job using the **net print** command. For more information, see the *LAN Manager Troubleshooting and Command Reference.*

Restarting a Print Job

You can restart a print job, printing it again from the beginning. This is useful if a job is interrupted by an error or printer problem.

To restart a print job using the Windows or Full Screen Admin Interface, follow these steps:

1 From the `View` menu, select `Printer queues.`

The `Print Queues` dialog box appears.

2 In the list box of print jobs, move the highlight to the number of the job you want to restart, then select the `Restart` command button.

3 On Windows clients, select the `OK` command button.

On MS OS/2 clients, select the `Done` command button.

Equivalent net Command. You can also restart a print job using the **net print** command. For more information, see the *LAN Manager Troubleshooting and Command Reference.*

Moving a Print Job in a Printer Queue

You can change the position of a print job already in a queue, moving it to the top or the bottom of the queue.

To move a print job to the first or last position in a queue using the Net Admin Interface, follow these steps:

1. From the `View` menu, select `Printer queues.`

   The `Print Queues` dialog box appears.

2. In the list box of print jobs, move the highlight to the number of the job you want to move, then select the `Zoom` command button.

   The `Printing Options for Job` dialog box appears.

3. Do *one* of the following:

   - To move the job to the top of the queue, select the `First in queue` option button.

     Note: If you make more than one job first in queue, the jobs will print in the order listed in the list box.

   - To move the job to the bottom of the queue, select the `Last in queue` option button.

     The job number of the print job changes.

4. Select the `OK` command button.

5. On Windows clients, select the `OK` command button.

   On MS OS/2 clients, select the `Done` command button.

Equivalent net Command. You can also move a print job to the first or last position in a queue using the **net print** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Deleting a Print Job

While a job is waiting in a printer queue, you, as administrator, can delete it. Non-administrative users can delete their own print jobs.

To delete a print job using the Net Admin Interface, follow these steps:

1 From the `View` menu, select `Printer queues.`

The `Print Queues` dialog box appears.

2 In the list box of print jobs, move the highlight to the number of the job you want to delete, then select the `Delete` command button.

A prompt for confirmation appears.

3 To confirm, select the `OK` command button.

4 On Windows clients, select the `OK` command button.

On MS OS/2 clients, select the `Done` command button.

Equivalent net Command. You can also delete a print job using the **net print** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Canceling a Print Job that Is Printing

To cancel a print job while it is printing using the Net Admin Interface, follow these steps:

1 From the `Status` menu, select `Device status.`

The `Shared Device Status` dialog box appears, with a list box of shared devices on the server, the status of each device, and the user currently using the device, if any.

2 In the list box of devices, move the highlight to the name of the printer whose current job you want to cancel, then select the `Kill` command button.

A request for confirmation appears.

3 To confirm, select the `OK` command button.

Printing stops and the job is deleted from the queue. The user who sent the job is notified that it has been canceled.

4 On Windows clients, select the `OK` command button.

On MS OS/2 clients, select the `Done` command button.

Equivalent net Command. You can also cancel a print job that is printing using the **net print** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Pausing and Continuing a Printer

You can pause an individual printer. When you are ready for a paused printer to resume printing, you can continue it. When you pause a printer, it cancels and re-queues its current job. It will not accept new jobs from any shared printer queue until you continue it.

Note: Pausing and then continuing a printer that is in an error condition will clear the error.

To pause or continue a printer using the Net Admin Interface, follow these steps:

1. From the `Status` menu, select `Device status.`

   The `Shared Device Status` dialog box appears, with a list box of shared devices on the server, the status of each device, and the user currently using the device, if any.

2. To pause a printer, in the list box of devices, move the highlight to the name of the printer, then select the `Pause` command button.

   The status message for the printer changes to `Paused.`

3. To continue a paused printer, in the list box, move the highlight to the name of the printer, then select the `Continue` command button.

   The status message for the printer changes to `Idle` or `Printing.`

4. On Windows clients, select the `OK` command button.

   On MS OS/2 clients, select the `Done` command button.

Equivalent net Commands. You can also pause or continue a printer using the **net pause** or **net continue** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Sending Printer Error Messages to a Print Operator

You might want LAN Manager to send printer error messages to the MS-DOS client that is used by the person responsible for adding paper and toner and removing paper jams.

To send printer error messages, follow these steps:

1. Add the username or computername to the `alertnames` keyword in the [*server*] section of the *lanman.ini* file on the server to which the printer is connected.
2. Increase the value for the `sizmessbuf` keyword in the [*messenger*] section of the *lanman.ini* file on the client to at least 512 bytes.

Chapter 7

Managing Server Operations

Overview

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

- using the Activity Monitor
- clearing or changing an administrative password
- using the administrative resources
- controlling services
- understanding the Alerter service
- auditing the server
- using the command-line administration utility
- understanding the error log
- replicating files and directories
- adjusting the server's security settings
- viewing and controlling sessions
- understanding the statistics display
- stopping and restarting the server
- synchronizing network clocks
- viewing available servers and resources

Activity Monitor

The Activity Monitor enables you to display statistics on total server usage and file and print service requests made by individual clients. The display of this information is updated every few seconds.

This section discusses how to use the Activity Monitor. It provides information on the following topics:

- accessing the screen
- understanding the screen layout
- understanding the contents of frames
- moving around the screen and using function keys
- selecting and releasing a client
- locking and unlocking the keyboard

Note: If the Activity Monitor's display has been corrupted by a message from the UNIX system or the Messenger service, you can refresh the screen by pressing the spacebar or CTRL - L.

Accessing the Activity Monitor

To access the Activity Monitor screen, you must use the UNIX System Administrative Interface, following these steps:

1 Access the `LAN Manager Server` menu, as described in Chapter 2.

2 Select `Display Activity Monitor.`

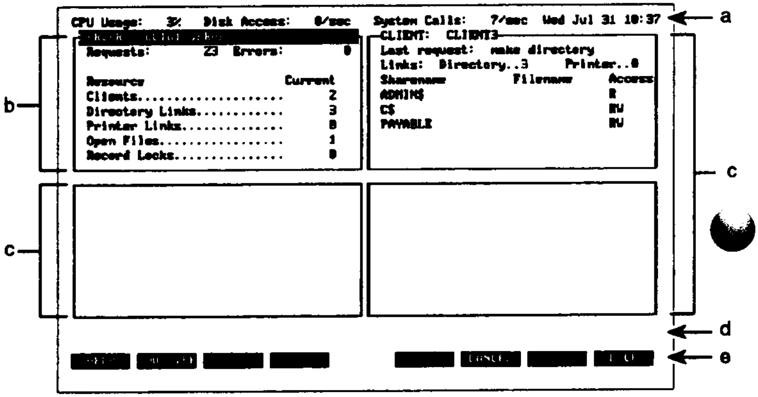
After a brief delay while the system gathers activity statistics, the Activity Monitor appears.

Understanding the Screen Layout

The Activity Monitor consists of four frames. When you first access the Activity Monitor, the frame in the upper left corner displays server data; the other frames display data for up to three of the clients that are currently linked to the server. You can use the WDW TYPE function key to change the kind of data (server or client) displayed in a frame.

The Activity Monitor screen is illustrated in Figure 7-1.

Figure 7-1: Activity Monitor



```
CPU Usage:   3%  Disk Access:    0/sec    System Calls:    7/sec  Wed Jul 31 10:37
                                           CLIENT:  CLIENT3
Requests:          23  Errors:         0   Last request:  make directory
                                           Links:  Directory..3     Printer..0
Resource                      Current      Sharename            Filename     Access
Clients....................         2      ADMIN$                            R
Directory Links............         3      C$                                RW
Printer Links..............         0      PAYABLE                           RW
Open Files.................         1
Record Locks...............         0
```

The screen includes the following parts:

a machine statistics

b server status frame

c client status frames

d message line

e function key labels

Clients are displayed by computername. If there are fewer than three active clients when you access the Activity Monitor, the additional frames are left blank. If more than three clients are linked to the server, the NEXTPAGE function key is displayed. You can use this key to display the next set of clients. If a displayed client disconnects from the network, the information for another client, the next in alphabetical order, is used to fill that frame.

Note: If a client is rebooted, there may be a delay of up to two minutes before the change is reflected in the Activity Monitor.

Understanding the Contents of Frames

This section explains the fields that appear on the Activity Monitor's two types of status frames:

- server status frame
- client status frame

Server Status Frame

The following information is displayed in a server status frame:

`Requests:` A counter that is updated each time the server receives and acknowledges a request from a client. The counter is reset to zero when it reaches 100 million.

`Errors:` A counter that is updated each time an error is recorded in the server's error log file. For example, if the server exceeds its maximum number of open files, this counter is updated.

`Resources:` The current number of active clients, directory links, printer links, open files, and record locks.

Client Status Frame

The following information is displayed in each client status frame:

`Last Request:` The last request that the client sent to the server.

`Directory:` The number of directory links between client and server.

`Printer:` The number of printer links between client and server.

Active directory links The `Sharename`, open `Filename` (if any), and file `Access` permissions are displayed under the appropriate column headings for active directory links.

If the client has one or more locks on a file, the filename is displayed in inverse video.

If there is more information than can be displayed at one time, the frame first displays directories in which the user has locked files, then open files without locks, and finally directory links without open files.

Active Printer Links

If the client has an active link to a shared printer queue, the queue's name is displayed.

For more information about printer and printer queue status, see Chapter 6.

Using the Keyboard

Use the keys listed in Table 7-1 to move from frame to frame, and to move around in a menu. The title bar at the top of the current frame (the frame in which you are located) appears in inverse video.

Table 7-1: Keys for Moving around the Screen and Selecting

Key	Function
↑	Move to upper frame or previous menu item
↓	Move to lower frame or next menu item
→	Move to frame on right
←	Move to frame on left
Tab	Move to next frame
Shift - Tab	Move to previous frame
↵	Select menu item

Function keys are associated with screen labels and are used to perform various actions. The screen label corresponding to each function key is described in Table 7-2.

Table 7-2: Function Keys

Label	Function
CANCEL	Exits from the Activity Monitor; exits from the current menu without making a selection; exits from help text.
CLIENT	Displays a pop-up menu of active clients. When you select from the menu, the information on that client is displayed in the current frame. The selected client information will occupy this frame until the client unlinks from the server or you select another client. The CLIENT label is displayed and active only when the current frame is a client frame. Updating is suspended while the menu is displayed.
HELP	Displays a frame with help text about the Activity Monitor. When you invoke help, only the CANCEL, NEXTPAGE, and PREVPAGE function keys are displayed and active.
LOCK	Locks the keyboard so that you can leave the Activity Monitor displayed but deny other users access to the UNIX System Administrative Interface, and therefore to system administration functions.

Table 7-2: *Continued*

Label	Function
	CAUTION: When you lock the keyboard, be sure that you are in a shell from which you cannot escape.
NEXTPAGE	Displays the next set of active clients (in alphabetical order). The clients currently on display are replaced, except for any clients you have selected using the CLIENT function key. (Selected client frames continue to be displayed until they are released.) The NEXTPAGE label is displayed and active only when there are more clients to display. When a help frame is displayed, this function key displays the next page of help text.
PREVPAGE	Display the previous set of three active clients. The clients currently on display are replaced, except for any clients you have selected using the CLIENT function key. The PREVPAGE label is displayed and active only when there is a previous set of clients to display. When a help frame is displayed, this function key displays the previous page of help text.

Table 7-2: *Continued*

Label	Function
UNLOCK	Unlocks the keyboard.
WDW TYPE	Displays a pop-up menu for converting a server frame to a client frame and vice versa. This function allows you to display information on four clients at a time, instead of the default of the server and three clients. Updating is suspended while the menu is displayed.

Selecting and Releasing a Client

You can select an active client for display in the current frame. The information on that client continues to occupy that frame even if you use the NEXTPAGE or PREVPAGE function key to display the next or previous set of clients.

To select a client for display, follow these steps:

1 Move to the frame in which you want the client information to be displayed.

Note: To display client information in the server frame, first use the WDW TYPE function key to convert it to a client frame.

2 Press the CLIENT function key.

The Clients menu appears.

3 Select the client you want to display.

The information on that client appears in the frame. This client's information will be displayed in this frame until you release the client or the client unlinks from the server. It also will be displayed in its usual place in the alphabetical listing if you use the PREVPAGE or NEXTPAGE function key to change the set of clients displayed.

4 To release a selected client, follow these steps:

a Press the CLIENT function key to display the client list.

b Select ANYCLIENT.

The selected client is removed from the frame and is replaced by the next client in the alphabetical list.

Locking and Unlocking the Keyboard

You may choose to leave the Activity Monitor on even when you are not present. However, doing so can leave the system administration functions accessible to other users. The LOCK and UNLOCK function keys allow you to lock the keyboard to prevent unauthorized access.

To lock the keyboard while the Activity Monitor is on, follow these steps:

Caution When you lock the keyboard, be sure that you are in a shell from which you cannot escape.

1 Press the LOCK function key.

The system prompts you for a password.

2 Type any password (that you will be able to remember) and press ↵.

Your entry is not displayed as you type.

The system prompts you to re-enter the password.

3 Type the password again and press ↵.

The system displays a confirmation that the keyboard is locked.

To unlock the keyboard, follow these steps:

1 Press the UNLOCK function key.

The system prompts you for a password.

2 Type the same password that you supplied when you locked the keyboard and press ↵.

The LOCKED message disappears, and the keyboard is unlocked.

Administrative Password

When the Server Program is installed, it creates an *admin* user account automatically, and prompts you for a password for this account. You can log on in the domain as *admin* and perform server management tasks such as adding users, sharing directories and printers, and managing printer queues.

If you forget the password for the *admin* account, you can reset it only through the UNIX System Administrative Interface, following these steps:

Many administrative tasks such as adding a new user transparently use the administrator's password. When you change your password, you must allow several minutes before doing administrative tasks since password propagation is not instantaneous.

Caution Only *one* person should use the UNIX System Administrative Interface at any given time; otherwise, data may be lost.

1 Access the `LAN Manager Server` menu, as described in Chapter 2.

2 Select `Set Administrative Password.`

A message is displayed, reminding you that selection of this menu item will clear the administrative password and allow you to set a new one, and prompting you for confirmation that you want to proceed.

3. To confirm, type `y` and press ↵.

   The `Password:` prompt appears.

4. Do *one* of the following:

   - To change the password, type a new one, then press ↵.
   - To clear the password, press ↵.

   The maximum length for a password is eight characters. The minimum length for a password is specified by the value of the `minpassword` keyword in the [*lmxserver*] section of the server's *lanman.ini* file.

   The `Re-enter password:` prompt appears.

5. Retype the password you entered in Step 4.

   The system displays a confirmation message.

6. Press ↵ to return to the `LAN Manager Server` menu.

Administrative Resources

LAN Manager automatically shares the administrative resources, *ADMIN$*, *IPC$*, and the disk administrative resource, *C$*. On a server running user-level security, you cannot unshare *ADMIN$* or *IPC$*. If you unshare *C$*, you can start sharing it again only by using the **net share** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

The *ADMIN$* resource controls access to server administration. To administer a server from a client, you do not have to make a connection to *ADMIN$*; when you begin a remote administration session, LAN Manager makes the connection automatically. However, you can make an explicit connection to a server's *ADMIN$* resource from a client. Making such a connection gives you access to all LAN Manager files and programs.

You can limit the number of users who can administer the server remotely by changing the `Max. users` value for *ADMIN$*. For instructions, see the next section.

The *IPC$* resource controls interprocess communication — that is, communication between different components of a program, different computers running parts of a single program, or two programs working together. In LAN Manager, interprocess communication occurs when a user or administrator performs one of the following actions:

- Views a list of a server's available resources.
- Administers the server remotely.
- Runs a distributed application. A distributed application is a software product (for example, SQL Server) designed to run on a network. In a distributed application, individual computers run programs that cooperate to get a single job done.

Users and administrators usually do not have to make an explicit connection to *IPC$*. When *IPC$* is needed, LAN Manager makes a connection automatically.

Changing Administrative Resource Options

You can change the configuration of an administrative resource that has been shared on a server by changing the following options:

- remark
- user limit
- who is permitted to use the resource — administrators only or all users

To change administrative resource options using the Net Admin Interface, follow these steps:

1. From the `View` menu, select `Shared resources.`

   The `Shared Resources` dialog box appears.
2. Mark the `Show hidden shares` check box.
3. In the list box, move the highlight to the administrative resource whose options you want to change, then select the `Zoom` command button.

   The `Information on the Special Resource` dialog box appears.

4 Change any options as desired, then select the `OK` command button.

The `Shared Resources` dialog box returns.

5 On Windows clients, select the `OK` command button.

On MS OS/2 clients, select the `Done` command button.

Equivalent net Command. You can also change administrative resource options using the **net share** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Controlling Services

You can pause, continue, start, and stop LAN Manager services. Note that LAN Manager, by default, starts the Alerter, Netlogon, and Server services.

Starting a Service

If LAN Manager does not automatically start a service, you can start any of the following services manually: Alerter, Net Logon, Netrun, NVAlert, RemoteBoot, Replicator, Server, SNMP, Timesource, UPS. To start a service, follow these steps:

Note: The Server service can only be started at the UNIX system console with the **net start** command. You must be logged on as `root`.

1. Log on with an account that has administrative privileges.
2. From the `Config` menu, select `Control services` and press ↵.

   The `LAN Manager Services` dialog box appears. The `Services in LANMAN.INI` column lists service names, with each name corresponding to the section of the *lanman.ini* file that controls the service. The `Status` column notes the services that are currently running. If a status is not displayed next to the service, the service is not running.

3 Select the service you would like to start and press [START].

The `Start a LAN Manager Service` dialog box appears.

4 Do one of the following:

- If you wish to start the service with the default settings, press [OK].
- If you wish to start the service with different settings, see the section "Adjusting Service Performance" later in this chapter. You cannot specify different settings for services on a UNIX system.

Note: When you use the **net start** command at a UNIX system server, the command ignores any option you enter. Instead, the service parameter is taken from the appropriate section of the *lanman.ini* file. If the parameter is not listed in the *lanman.ini* file, a default value is used. If you wish to modify a parameter, you must modify the *lanman.ini* file first and then enter the **net start** command.

5 On Windows clients, press [OK].

On MS OS/2 clients, press [DONE].

Equivalent net Command. You can also start a service using the **net start** command. For more information, see the *LAN Manager Troubleshooting and Command Reference.*

Pausing A Service

Pausing suspends the following services: Netlogon, Netrun, Print, Server, and SNMP. Unlike stopping services, pausing does not cancel resource sharing or connections, or change settings associated with the service.

With the exception of the Print service, pausing a service allows the current job at each service to complete before pausing begins. Pausing the Print service stops the current jobs.

To pause the Server service, you must have administrative or server operator privilege. Pausing the Server service prevents users from making new connections to the server's shared resources; however, those users who have already connected to shared resources before pausing was invoked can continue to use the resources during pausing.

To pause a service, follow these steps:

1 From the `Config` menu, select `Control services` and press [↵].

The `LAN Manager Services` dialog box appears.

2 Select the service that you wish to pause and press [PAUSE].

Note: Some services cannot be paused or continued. If you try to select these services, [PAUSE] will dim.

3 On Windows clients, press [OK].

On MS OS/2 clients, press [DONE].

Equivalent net Command. You can also pause a service using the **net pause** command. For more information, see the *LAN Manager Troubleshooting and Command Reference.*

Continuing a Service

When you continue a service, you restore sharing, connections, and other associated services that were previously paused. The following services can be continued: Netlogon, Netrun, Print, Server, and SNMP.

Follow these steps to continue a service.

1. From the `Config` menu, select `Control services` and press ↵.

   The `LAN Manager Services` dialog box appears.

2. Select the service that you wish to continue and press CONTINUE.

3. On Windows clients, press OK.

   On MS OS/2 clients, press DONE.

Equivalent net Command. You can also continue a service using the **net continue** command. For more information, see the *LAN Manager Troubleshooting and Command Reference.*

Stopping A Service

Stopping a service disables all features provided by that service. Stopping a service can cancel resource sharing and connections. The following services can be stopped: Netlogon, Netrun, Print, Server, and SNMP.

Caution Do **not** stop a LAN Manager server by pressing Ctrl + Alt + Del. Before you shut down a server (especially a primary domain controller, a backup domain controller, or a member server using logon security) be sure to stop all LAN Manager services. Then follow the appropriate UNIX system procedure before restarting the server or turning it off. Data can be lost if you shut down a server without following these steps.

Before LAN Manager stops a service, it displays a message box confirming your choice.

Stopping the Server service cancels any shared resources and other users' connections to shared resources. Only an individual with administrative privilege can stop the Server service.

Note: Before stopping the Server service, you should first pause the service and send a message to users connected to the server's shared resources, warning them that the Server service will be stopped. For information about sending messages, see the *LAN Manager User's Guide for MS-DOS* or the *LAN Manager User's Guide for MS OS/2.*

You must have administrative or server operator privilege to stop the following services:

- Alerter
- Netlogon

- Netrun
- NValert
- Server
- SNMP
- Timesource
- UPS

To stop an individual service, follow these steps:

1 From the `Config` menu, select `Control services` and press ↵.

The `LAN Manager Services` dialog box appears.

2 Select the service you wish to stop and press STOP.

The system asks you if you wish to stop the service.

3 Press OK.

Equivalent net Command. You can also stop a service using the **net stop** command. For more information, see the *LAN Manager Troubleshooting and Command Reference.*

Adjusting Service Performance

Each service has parameters that affect the way the service runs. All of these parameters can be altered, either permanently (the specified values take effect each time you start the service) or temporarily (the specified values are in effect only until you stop and restart the service).

Permanent Changes

To make a permanent change, you must enter the parameter with the value you want in the *lanman.ini* file for the server or client.

Some parameters are written into the *lanman.ini* file when you install LAN Manager. For example, the `srvservices` keyword in the [*server*] section of *lanman.ini* specifies the services that will be started when the Server service is started.

Most parameters have default values. If a parameter is not listed in the *lanman.ini* file, the default value will be used.

Some values are autotuned, or adjusted automatically. You can override these values by adding them to *lanman.ini*, but this will defeat the autotuning feature.

The *lanman.ini* file is in the *lanman* directory. For a complete discussion of the *lanman.ini* file, see Appendix B.

Temporary Changes

For each service parameter, there is a corresponding option to the **net start** command. To make a temporary change in a service's parameters, you must include the appropriate options when you start the service. The new value will remain in effect for as long as the service is running. When you stop and restart the service, the default value, or the value specified in *lanman.ini* is restored.

Note: When you use the **net start** command at a UNIX system server, the command ignores any option you enter. Instead, the service parameter is taken from the appropriate section of the *lanman.ini* file. If the parameter is not listed in the *lanman.ini* file, a default value is used. If you wish to modify a parameter, you must modify the *lanman.ini* file first and then enter the **net start** command.

Specifying Parameters When Starting a Service

To set parameters for a UNIX system server, you must edit the *lanman.ini* file on the server before you start the service.

To set parameters on a client or on an MS OS/2 server when starting a service, follow these steps:

1 From the `Config` menu, select `Control services` and press ↵.

The `LAN Manager Services` dialog box appears.

2 Select the service you want to start and press START .

The `Start a LAN Manager Service` dialog box appears. The `Option` column displays the entries in the *lanman.ini* file that control the service. The `Value` column displays the current values.

3 Either select an option or type the name of the option you wish to change in the `Option` box. Press ↵.

4 Type the value you wish to assign to the option in the `Value` box and press SET .

5 Do one of the following:

- To continue without changing another option, go to Step 6.
- To change another option, repeat Steps 3 and 4.
- To restore the default setting for an option, select the option and press RESET .
- To restore all of the default settings, press RESET ALL .

6 Press OK .

If you specify an illegal value, LAN Manager displays an error message and the `Start a LAN Manager Service` dialog box.

Starting and Stopping Administrative Services - Alternative Method

You can also start and stop the Server service and other administrative services using the following alternative procedure. When you stop and restart administrative services, the values set by the autotuning feature take effect (unless you have overridden them with entries in the *lanman.ini* file).

Note: For other service parameters, LAN Manager uses default values, or the values named in the *lanman.ini* file to configure the service.

To stop and start administrative services, follow these steps:

1 From the `Config` menu, select `Server options` and press ↵.

The `Set Configuration for Server` dialog box appears. The `Start server services` check boxes control the following services: Alerter, Netrun, Netlogon, Remoteboot, Replicator, and Server.

If the check box next to the service is selected, the service is running. If the check box is blank, the service is not running.

2 Select or clear the appropriate check box and press **OK** .

Alerter Service

Under certain circumstances, such as when a user's quota of disk space is almost full, the Alerter service sends messages called alerts. The receiving computer must be running the Messenger service to receive alerts. The `sizmessbuf` keyword in the [*messenger*] section of the client's *lanman.ini* file must specify at least 512 Kbytes. On either an MS-DOS or an MS OS/2 client, if the NetPopup service is running, the alert is displayed on the screen. On a Windows client, if the Messenger and WinPopup services are running and an alert occurs, the WinPopup icon appears. Click on the icon to see the alert.

There are three classes of alerts:

- **Error alerts** are messages about network or system errors. These messages are recorded in the error log. For more information about the error log, see the section "Error Log" later in this chapter.
- **Print alerts** relate to printer events, such as when a print job is completed, or the printer is out of paper. A print alert is sent to the users listed as the value of the `alertnames` keyword in the server's *lanman.ini* file.
- **Admin alerts** are messages about server and resource use, and are sent only to those users specified by the `alertnames` keyword in the [*server*] section of the *lanman.ini* file. For example, an admin alert is sent when the maximum allowed number of users is using a resource, or too many logon violations have occurred.

For some alert conditions, you can specify when LAN Manager should notify you. For example, you can specify that an alert should be sent when a user makes 10 unsuccessful attempts to log on.

The keywords in the [*server*] section of the server's *lanman.ini* file control when and to whom the server sends alerts and the alert conditions to be checked. These keywords are listed in Table 7-3. For additional information, see Appendix B.

Table 7-3: Alert Keywords

Keyword	Description
`accessalert`	sets the number of resource access violations that will trigger an alert. This keyword applies only to servers running user-level security. The range is 0 to unlimited; the default is 5.
`alertnames`	lists the users to receive administrative and printer alerts. The default is `admin`.
`erroralert`	sets the number of errors that will trigger an alert. The range is 0 to unlimited; the default is 5.
`logonalert`	sets the number of logon violations that will trigger an alert. The range is 0 to unlimited; the default is 5.

Changing the Alertnames List

Any changes you make to the list of usernames to receive alerts take effect immediately. To change the alertnames list using the Net Admin Interface, follow these steps:

1. From the `Config` menu, select `Server options.`

   The `Set Configuration for Server` dialog box appears.

2. In the `Send alerts to` text box, type a list of username to receive alerts, separated by commas.
3. Select the `OK` command button.

Equivalent net Command. You can also change the Alertnames using the **net config server** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Auditing the Server

LAN Manager audits the network by recording events such as valid and invalid logon attempts and events related to resource use, such as the opening of files in shared directories. When auditing is enabled, each time one of these events occurs it is logged in the server's audit trail. Audit records are useful for examining how often a resource is used and whether access permissions set for the resources are appropriate.

Auditing is available for servers running either user-level or share-level security. Keywords in the [*server*] section of the *lanman.ini* file and settings on individual resources under user-level security determine when auditing is enabled and what kinds of events are audited. By default, auditing is disabled.

Defining Audited Events

The `auditing` and `noauditing` keywords in the [*server*] section of the *lanman.ini* file control which events are audited. The `auditing` keyword can have a value of `yes` (enable auditing), `no` (disable auditing), or a list of events to be audited. The value of the `noauditing` can have the same values: `yes` (disable auditing), `no` (enable auditing), or a list of events not to be audited.

Auditable events differ for servers running user-level and share-level security. Because you do not set resource permissions for each group or user, auditable events under share-level security are limited to the starting and stopping of services, starting and ending of a session at a server, and use of resources.

Table 7-4 lists the values that can be included in a list of events for the auditing and noauditing keywords under each security mode.

Table 7-4: Audited Events

Event	Description
User- and Share-Level Security	
service	Record each time a service is started or stopped.
sesslogon	Record all attempts to log on or off this server.
goodsesslogon	Record successful attempts to log on or off this server.
badsesslogon	Record unsuccessful attempts to log on or off this server.
use	Record all attempts to use shared resources.
gooduse	Record successful attempts to use shared resources. However, gooduse is not audited if a shared resource allows an unlimited number of users.
baduse	Record unsuccessful attempts to use shared resources.
User-Level Security Only	
logon	Record all logon attempts (netlogon + sesslogon).
logonlimit	Record each time a user exceeds his or her logon hours.
netlogon	Record all attempts to log on to the network.
goodnetlogon	Record successful attempts to log on to the network.
badnetlogon	Record unsuccessful attempts to log on to the network.
permissions	Record changes to resource access permissions.
resource	Record all attempts to use shared resources.
userlist	Record changes to the user accounts database.

For example, to audit only logon attempts, in *lanman.ini*, enter `auditing=logon`.

Another way to audit only particular events is to enter `auditing=yes` and list events that are not to be audited in the `noauditing` keyword, in which case all events except the `noauditing` events are audited.

For example, to audit all events except logon attempts and the starting and stopping of services, enter `auditing=yes` and `noauditing=logon,service`.

When you change the `auditing` and/or `noauditing` keywords in *lanman.ini*, you must stop and restart the server for the changes to take effect. For instructions on stopping and restarting the server, see the section "Stopping and Restarting the Server" later in this chapter.

You can set the size of the audit trail with the `maxauditlog` keyword in the [*server*] section of the *lanman.ini* file, or temporarily with the **/maxauditlog** parameter of the **net config server** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*. You may want to reduce the size of the trail if you do not need extensive audit information. The range, in KBytes, is 0 to unlimited; the default is 100 KBytes.

Changing Audited Events

To change audited events using the Net Admin Interface, follow these steps:

1 From the `Config` menu, select `Server options`.

The `Set Configuration for Server` dialog box appears.

2 Select the `Auditing` command button.

The `Auditing the Server` dialog box appears.

3 Mark the `Auditing enabled` check box.

4 In the `Audited events` check boxes, mark the events you want to audit.

Note: These check boxes define sets of values for the `auditing` and `noauditing` keywords. To specify a customized list of the values shown in Table 7-4, edit the *lanman.ini* file as described in the previous section.

5 Select the `OK` command button.

The `Set Configuration for Server` dialog box returns.

6 On Windows clients, select the `OK` command button.

On MS OS/2 clients, select the `Done` command button.

Equivalent net Command. You can also change audited events using the **net config server** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Viewing, Saving, and Clearing the Audit Trail

By default, the audit trail is stored as a file named *net.aud* in the server's *lanman/logs* directory. The Net Admin Interfaces also create two auxiliary files in *lanman/logs*:

- When you clear the audit trail, the contents of *net.aud* are moved to a backup audit file. On Windows clients, this file is called *net.bak.* On On MS OS/2 clients, it is called *audit.bak.* The *net.aud* file is cleared. Any previous contents of the backup audit file are overwritten.
- When you save the audit trail, the contents of *net.aud* are copied to a backup audit trail file. On Windows clients, this file is called *net.sav.* On MS OS/2 clients, it is called *audit.sav.* The *net.aud* file is not cleared. Any previous contents of the backup audit trail file are overwritten.

On Windows clients, to keep a permanent record, copy *net.sav* or *net.bak* to another file.

On MS OS/2 clients, to keep a permanent record, copy *audit.sav* or *audit.bak* to another file.

On a server running share-level security, the audit trail can provide information about when a service has been started or stopped, when a user has started or ended a session at the server, and when a resource has been accessed.

On a server running user-level security, the audit trail provides the following information about each audited event:

- The username of the user who caused the event. Asterisks (***) appear if no username is available.
- The kind of event, which is one of the following:

  `Server` events such as starting and stopping the server

`Session`	sessions started with the server
`Share`	events such as starting and stopping the sharing of resources
`Access`	resource access
`Access Denied`	failed attempts to access a resource

- The date and time of the audited event.

Procedure. To view, save, and clear the audit trail using the Net Admin Interface, follow these steps:

Note: If your audit log is very large (larger than 800K), you might be unable to view it from the Net Admin Interface screen. However, you can always view it by using the **net audit** command.

1 To view the audit trail, from the `Status` menu, select `Audit trail.`

On Windows clients, the `View Network Audit Trail` dialog box appears.

On MS OS/2 clients, the `Network Audit Trail` dialog box appears.

2 Do *one or more* of the following, as appropriate:

- To exit without taking further action, go on to Step 5.

- To save the audit trail, go on to Step 3.
- To clear the audit trail, go on to Step 4.

3 To save the contents of the audit trail in the *audit.sav* file, follow these steps:

a Select the `Save` command button.

A request for confirmation appears.

b To confirm on Windows clients, select the `Yes` command button.

To confirm on MS OS/2 clients, select the `OK` command button.

4 To clear the audit trail and start a new audit record, follow these steps:

a Select the `Clear` command button.

A request for confirmation appears.

b To confirm on Windows clients, select the `Yes` command button.

To confirm on MS OS/2 clients, select the `OK` command button.

5 Select the `Done` command button.

Equivalent net Command. You can also view or clear the audit trail using the **net audit** command. You cannot save the audit trail using **net audit**. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Command-Line Administration Utility

The UNIX System Administrative Interface provides a command-line administration utility to administer LAN Manager servers using appropriate **net** commands.

To run the command-line administration utility using the UNIX System Administrative Interface, follow these steps:

Caution Only *one* person should use the UNIX System Administrative Interface at any given time; otherwise, data may be lost.

1. Access the `LAN Manager Server` menu, as described in Chapter 2.
2. Select `Run Command-Line Administration Utility.`

   The `Run Command-Line Admin` form appears.
3. In the `Servername:` field, type the name of the server you want to administer, in the format *uname*`.`**`serve`**

   Replace *uname* with the server's UNIX system name.

4. In the `Username:` field, type an appropriate username, depending on the kind of server you want to administer, as follows:

   - If the server is running user-level security or an earlier version of the Server Program, type **`admin`** and press ↵.
   - If the server is running share-level security, type any name consisting of characters valid for a username.

5. In the `Password:` field, type the appropriate password, depending on the kind of server you want to administer, as follows:

   - If the server is running user-level security or an earlier version of the Server Program, type the password for the username you entered in Step 4.
   - If the server is running share-level security, type the password for the *ADMIN$* directory.

   The Command Line Net Interface's `[\\`*uname*.**serve**`]` prompt appears. At this prompt, you can type the appropriate **net** commands to administer the server.

6. To return to the `LAN Manager Server` menu, type **`exit`** and press ↵.

   The `LAN Manager Server` menu returns.

Error Log

The error log's record of client and server errors is kept in the *net.err* file in the server's *lanman/logs* directory. On Windows clients, if the Messenger and WinPopup services are running, some errors also cause the WinPopup icon to appear. Click on the icon to see the error message. On MS OS/2 clients, if the Messenger and NetPopup services are running, some errors also appear on the screen as alerts.

If you are searching for the cause of a problem and cannot find any relevant messages, you can look for evidence in the audit trail, as described in the section "Auditing the Server" earlier in this chapter. For example, an incorrect password attempt is recorded in the audit trail rather than the error log.

The error log displays the following information, listing errors in chronological order, from oldest to newest:

- service error
- error number
- date and time when the error occurred

The Net Admin Interfaces create two auxiliary files in the *lanman/logs* directory:

- When you clear the error log, the contents of *net.err* are moved to the *error.bak* file. The *net.err* file is cleared. Any previous contents of *error.bak* are overwritten.

- When you save the error log, the contents of *net.err* are copied to the *error.sav* file. The *net.err* file is not cleared. Any previous contents of *error.sav* are overwritten.

To keep a permanent record, copy *error.sav* or *error.bak* to another file.

Procedure. To view, save, or clear the error log using the Net Admin Interface, follow these steps:

1 From the `Status` menu, select `Error log`.

  The `Network Error Log` dialog box appears.

2 Do *one or more* of the following, as appropriate:

  - To view the error log, go on to Step 3.
  - To save the error log, go on to Step 4.
  - To clear the error log, go on to Step 5.

3 To get more information about an error, follow these steps:

  a In the list box of errors, move the highlight to a selected error, then select the `Zoom` command button.

    The `Error Log Record` dialog box appears.

  b On Windows clients, select the `OK` command button.

    On MS OS/2 clients, select the `Done` command button.

  c Go on to Step 6.

4 To save the contents of the error log in the *error.sav* file, follow these steps:

  a Select the `Save` command button.

  A request for confirmation appears.

  b To confirm, select the `OK` command button.

  c Go on to Step 6.

5 To clear the error log, follow these steps:

  a Select the `Clear` command button.

  A request for confirmation appears.

  b To confirm, select the `OK` command button.

  c Go on to Step 6.

6 On Windows clients, select the `OK` command button.

On MS OS/2 clients, select the `Done` command button.

Equivalent net Command

You can also view or clear the error log using the **net error** command. You cannot save the error log using **net error**. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Replicating Files and Directories

The Replicator service allows you to maintain identical sets of files and directories on different servers. Replication simplifies the task of updating and coordinating files. If users need access to specific files, you can update the files on one server and let replication take care of updating them on other clients and servers.

The Replicator service can replicate administrative and application program source files, including configuration profiles and application directories. For example, you can use this service to maintain a set of identical logon scripts on all servers running user-level security that are used as logon servers in a domain.

Replication is controlled by options you set in the *lanman.ini* file as described in the following section.

How Replication Works

To replicate a set of files and directories on several computers, you must designate a server as an **export server**, which is where you maintain the master set of files and directories. You then designate servers and clients that receive replicated files as **import servers**.

A network can have any number of export and import servers. A server can be both an export and an import server. Clients can be configured only as import servers.

All files and directories that are to be replicated are kept in the export server's *export* directory. Import servers must have a corresponding *import* directory with exactly the same subdirectory structure as that of the export directory. An export server replicates only those subdirectories for which there are corresponding directories under the import directory on the import server.

Export servers can replicate directory trees with as many as 32 levels. Each directory can contain as many as 2000 files.

The Replicator service monitors the export directory. When you change a file, or add or delete a directory or file in the export directory, the Replicator service makes the equivalent change in the corresponding import directories on all import servers. Files cannot be replicated when they are open.

From an export server, you can target replication — replicating to some files on one group of import servers and to other files on another group — by creating subdirectories in the export directory. Files in the export directory itself are not replicated. Export servers replicate only subdirectories for which there is a matching directory directly under the import directory on the import server.

The import directory path can be either a local path or the network path of a remote server. To replicate files locally, specify both an export and import directory path on the export server. This creates mirror copies of the data and is useful for updating shared directories on the export server.

Using a remote import directory path has the effect of "pushing" data changes to a remote target. This feature can be used to replicate data to LAN Manager servers prior to version 2.0, which do not support the Replicator service. For example, if you specify **`importpath=\\lm1server\public\replimp`** in a LAN Manager 2.2 server's *lanman.ini* file where **`\\lm1server`** is a pre-2.0 LAN Manager server, files will be replicated to **`\\lm1server`**.

Note: Because import servers can synchronize with only one export server for a specific directory, two export servers cannot replicate the same directories and files to the same import servers.

The repl.ini File

Replication is controlled by options that you can set in the [*replicator*] section of the *lanman.ini* file.

In each first-level subdirectory of the export directory, you can create a *repl.ini* file, which controls how much of that subdirectory is replicated, and under what conditions. The *repl.ini* file contains the keywords `extent` and `integrity`, each with the value `tree` or `file`.

`extent` specifies the extent of replication under the subdirectory containing *repl.ini*. If `extent=tree`, all files and subdirectories below the subdirectory are replicated. If `extent=file`, only files directly under the subdirectory are replicated.

`integrity`

sets a stability requirement for replication. If `integrity=tree`, all files and subdirectories must be stable (unchanged) for a specified interval (set by the `guardtime` keyword of the *lanman.ini* file) before they can be replicated. If `integrity=file`, files and subdirectories can be replicated as soon as they are changed.

If you do not create a *repl.ini* file, the Replicator service uses the following default values:

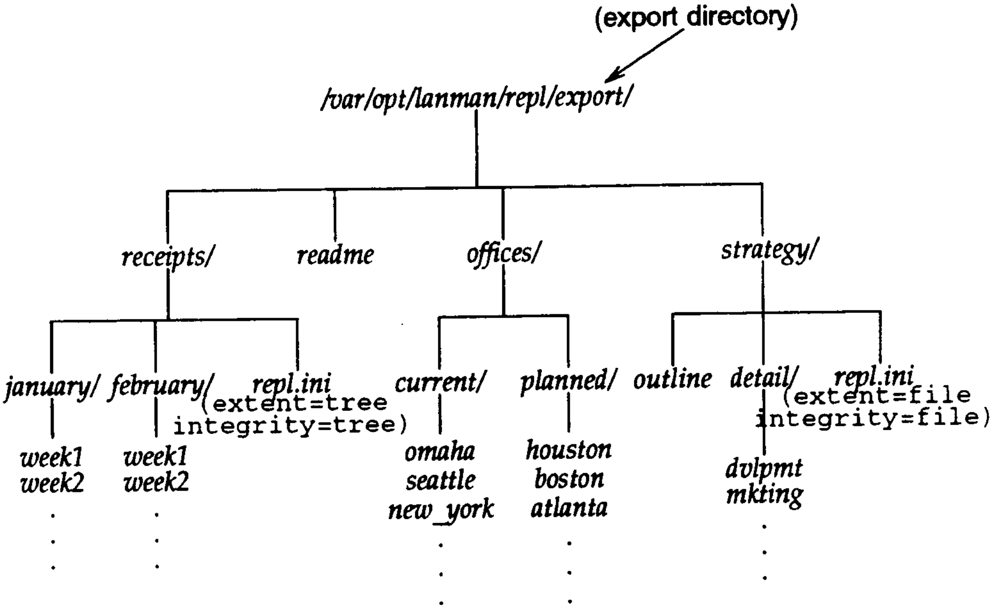
```
extent=tree
integrity=file
```

(Each keyword must be on a line by itself.)

Figure 7-2 is an example illustrating the structure of a typical export directory that replicates three subdirectories. (Directories are shown with a trailing slash (/), while files are not.) In this example, files and directories are replicated as follows:

- The *readme* file, which is not in a subdirectory of the export directory, is not replicated.
- The entire *receipts* directory tree is replicated (`extent=tree`), but only after all files in the tree are stable for the specified interval (`integrity=tree`).
- In the *offices* subdirectory, where there is no *repl.ini* file, the defaults are in effect: the entire directory tree is replicated (`extent=tree`), and files can be replicated while other files are open or being changed (`integrity=file`).
- In the *strategy* subdirectory, the *outline* file is replicated but the *detail* subdirectory is not (`extent=file`).

Figure 7-2: Sample Export Directory



The following sections provide procedures for preparing an export server to send replicas and for preparing an import server to receive replicated directories.

Preparing an Export Server

For information about exporting logon scripts for user-level security, see Chapter 4.

Use the following procedure to prepare an export server to send replicated files to import servers and clients using the Replicator service. To complete this procedure, you must first edit the [*replicator*] section of the *lanman.ini* file, create an export directory tree, and then start the Replicator service.

If you will be using the Replicator service on an ongoing basis, you should imbede the Replicator in the [*srvservices*] keyword in the [*server*] section of the *lanman.ini* file.

To prepare an export server for replication, follow these steps:

1 Edit the following keywords in the [*replicator*] section of the *lanman.ini* file to the following values:

- `replicate=export`

  or, to configure the server as both an export and import server,

  `replicate=both`

- `exportpath=`*path*

  Replace *path* with the path to the server's export directory tree, relative to *lanman*. By default, the Replicator service expects this path to be `repl/export`.

- `exportlist=`*servers*

  Replace *servers* with a list of up to 32 import servers and/or domains, separated by semicolons (;). When specifying a computername, do not include the two backslashes (\\ ) at the beginning of the name.

The default is the export server's domain.

- `interval=`*number*

  Replace *number* with the interval (in minutes) at which the Replicator service is to check the export directory for changes. The range is 1 to 60; the default is 30.

- `guardtime=`*number*

  Replace *number* with the interval (in minutes) that the export directory must be stable (no file changes) before it can be replicated to import servers. The range is 0 to half the value of `interval`; the default is 2.

- `pulse=`*number*

  Replace *number* with a number specifying how often the export server sends update messages to an import server when no change occurs. This value represents multiples of the value of `interval`. The range is 1 to 10; the default is 3.

- `random=`*number*

  Replace *number* with a number specifying the maximum number of seconds import servers can wait before accepting file updates. The range is 1 to 120; the default is 60. Each server in the domain should have a different value set to avoid simultaneous updates.

Note: Except for `replicate`, each of these keywords pertains either to export or import servers, but not to both.

2 Create the export directory specified by the `exportpath` keyword.

3 Under the export directory, follow these steps:

   a Create a subdirectory for each set of files that you want to replicate.

   b Copy the files to be replicated into each subdirectory.

   c If you do not want to accept the default *repl.ini* settings (`extent=tree; integrity=file`) for any subdirectory, create a *repl.ini* file in that subdirectory with the desired settings.

4 In the [*server*] section of the *lanman.ini* file, add **`replicator`** to the list of services in the `srvservices` keyword.

5 Stop and restart the Replicator service for the changes to take effect. For instructions on stopping and restarting the Replicator service, see the section "Controlling Services".

Assigning Permissions for Replication

To replicate files and directories to an import server, the Replicator service must be able to access the export directory tree on behalf of the import server. Regardless of whether the import server has user-level or share-level security, the import server must have RA (read and change attribute) access permissions for the export directory tree.

Import Servers with User-Level Security. On import servers with user-level security, you have the following two ways to grant access to the export directory tree:

- In the [*replicator*] section of the import server's *lanman.ini* file, set the `tryuser` keyword to `yes`. When this keyword is set to `yes`, the Replicator service tries to replicate files using the permissions for the user logged on at the import server. For replication to occur, the user must have an account for the export server and must have RA (read and change attributes) permissions for the *repl\export* directory.

  If `tryuser` is set to `no`, the user's permission will not allow replication and the Replicator service will automatically try the second method.
- In the [*replicator*] section of the import server's *lanman.ini* file, set the `logon` keyword to *username*, where *username* is the name of a user account that has RA permissions for the *repl\export* directory on the export server. Set the `password` keyword to that account's password on the export server. For replication to occur, no users can be logged on at the import server.

Creating a Default Access Account for Import Servers with User-Level Security. The simplest way to provide access to multiple import servers with user-level security is to create a group on the export server, assigning it RA permissions for the export directory tree. This group must include an account for each import server.

To create a default access account, follow these steps:

1 On the export server, create the group *rep*.

2 Create a user account for the computername of each import server, and add these accounts to the *rep* group.

   For example, for the computername *finance*, you might create the user account *finance_repl*.

   Do not simply copy the computername of the import server.

   Use **net user /passwordreq:no** command to specify that passwords are not required for these accounts.

   Note: To log on to an account with a zero-length password without being prompted for the password, include empty double quotation marks (" ") in place of the password on the command line. For example, type `net logon bestuser ""`.

3 Assign the *rep* group RA permissions for the export directory tree.

Import Servers with Share-Level Security. On servers with share-level security, the export directory tree (*lanman**repl**export*) is automatically shared as *repl$* with RA permissions when you start the Replicator service. It is shared without a password.

Preparing an Import Server

To prepare an import server to receive replicated files, you must edit the [*replicator*] section of the *lanman.ini* file, set the Replicator service to start automatically, and then create an import directory tree.

To prepare an import server, follow these steps:

Note: Except for `replicate`, each of these keywords pertains either to export or import servers, but not to both.

1 Change the following keywords in the [*replicator*] section of the *lanman.ini* file to the values shown, using **`srvconfig -s replicator,`** *keyword=value* .

- `replicate=import`

  or, to configure the server as both an export and import server,

  `replicate=both`

- `importpath=`*path*

  Replace *path* with the path to the server's import directory tree, relative to *lanman*. By default, the Replicator service expects this path to be `repl/import`.

- `importlist=`*servers*

  Replace *servers* with a list of up to 32 export servers and domains, separated by semicolons (;). When specifying a computername, do not include the two backslashes (\\ ) at the beginning of the name. The default is the import server's domain.

- `tryuser=no`

  This keyword indicates whether the Replicator service should try to logon as the `tryuser=no` name. The default is `no` and it is recommended that you use the default.

- `logon`

  This keyword specifies a username for the Replicator service to use when logging on to the export server. The default is `guest` and it is recommended that you use the default.

- `password`

  This keyword specifies the password for the Replicator service to use with the `logon` keyword. The default is `no` and it is recommended that you use the default.

2 Create the import directory tree specified by the `importpath` keyword.

3 Within the import directory tree, create a subdirectory with the same name as each first-level subdirectory that you want to replicate in the export server's export directory tree.

  For example, to replicate the directory tree illustrated in Figure 7-2, create the first-level directories *receipts* and *offices*. When `extent=tree` (the default), the Replicator service automatically creates the necessary subdirectories within those directories.

4 Add **`replicator`** to the list of services in the `srvservices` keyword in the [*server*] section of the *lanman.ini* file.

5 Stop and restart the Replicator service for the changes to take effect. For instructions on stopping and restarting the Replicator service, see the section "Controlling Services."

Maintaining Replication

Users should not change any of the files in import directories, because these files are overwritten when the Replicator service updates the import directory.

To ensure that files and directories in the export directory are not replicated while they are being updated, in a first-level subdirectory under the export directory, create an empty file named *userlock*.

In the *repl* directory tree illustrated in Figure 7-2, putting a *userlock* file in the *receipts* subdirectory would prevent replication of all files in the *receipts*, *january*, and *february* subdirectories. *userlock* files are only in effect when `integrity=tree` in the *repl.ini* file. If `integrity=file`, the *userlock* file is ignored.

To indicate the import directory's replication status, the Replicator service puts one of the following signal files in each first-level subdirectory:

ok.rp$ The directory is receiving regular updates from an export server, and the data is identical to that of the export. The date stamp on this file is set to the last time an update was received.

no_mastr.rp$ The directory is not receiving updates — the export server either is not running or has stopped exporting this directory. This file is also put in a newly created import directory when the Replicator service first starts.

no_sync.rp$ The directory is receiving updates from an export server, but the data is not up to date. The reason could be a communication failure, the presence of open files on the import or export server, the import server not having access permissions at the export server, or failure of the export server. The date stamp on this file is set to the time the directory first became out of date.

Stopping Replication

You can stop replication of files at any time on either an export server or an import server.

To stop replication, follow these steps:

1 On an export server, do *one* of the following:

- Stop the Replicator service. To do so, follow these steps:

  a Change the `replicate` keyword in the *lanman.ini* file to a null value:

  ```
  srvconfig -s replicator,
  replicate=
  ```

  b Stop and restart the Replicator service, as described in the section "Controlling Services".

- Delete files from the export directory.
- Delete the first-level subdirectory that you no longer want to export.
- Create a file named *userlock* in each subdirectory that you want to temporarily stop replicating.

2 On an import server, stop the Replicator service. To do so, follow these steps:

   a Change the `replicate` keyword in the *lanman.ini* file to a null value:
   ```
   srvconfig -s replicator,
   replicate=
   ```

   b Stop and restart the server, as described in the section "Stopping and Restarting the Server" later in this chapter.

Server Security Settings

The server's security settings define the rules for changing user account passwords on the server, how the server handles logons outside of specified logon hours, and the number of failed logon attempts that a user is allowed before the account is locked out.

To change security settings using the Net Admin Interface, follow these steps:

1. From the `Accounts` menu, select `Security settings.`

   The `Security Settings` dialog box appears, showing the current security settings, as well as the server's role. For more information about server roles, see Chapter 3.

2. In the `Minimum password length` text box, type a value in the range **`0`** through **`14`** (characters). The default is 6.

3. In the `Password uniqueness` text box, type a value in the range **`0`** through **`48`** (previous passwords that cannot be reused). The default is 5.

4. In the `Minimum password age` text box, type a value in the range **`0`** through **`49710`** (days). The default is 0.

5 From the `Maximum password age` option buttons, select *one* of the following:

- `No limit`
- `Valid for`

  If you select this button, in the adjacent text box, type a value in the range **1** through **49710** (days). The default is no limit. (LAN Manager prevents you from specifying a maximum password age less than the minimum password age.)

6 From the `Force logoff` option buttons, select *one* of the following:

- `Immediately` to log users off as soon as their logon hours or accounts expire.
- `Never` to allow users to remain logged on despite their logon limits.
- `After` to force users to log off a specified interval after expiration.

  If you select this button, in the adjacent text box, type a value in the range **1** through **11574** (seconds — the maximum value is slightly over 3 hours).

7 From the Lock-out accounts option button, select *one* of the following:

- After to specify the maximum number of failed logon attempts a user is allowed before the account is locked out.

  If you select this button, in the adjacent text box, type a value.

- Never to specify no maximum.

  The default is no maximum.

8 Select the OK command button.

Equivalent net Command. You can also change security settings using the **net accounts** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Sessions

Each time a client links to a server, a session is established between the client and server. A session starts when a user on a client makes a connection to a server, such as with the **net use** command. For a server running user-level security, a session is established when the server's user accounts database validates the user's password and username. For a server running share-level security, a session is established when the user makes a connection to a resource on a server.

An administrator can specify the maximum number of sessions a server can support, view and control users' sessions, and close files opened on a session. Information on sessions is useful for gauging the server's work load.

Table 7-5 lists the keywords in the [*server*] section of the server's *lanman.ini* file that govern sessions.

Table 7-5: Session Keywords

Keyword	Description
`autodisconnect`	is the interval that the server waits for activity before disconnecting an inactive session. The range is 0 to 3600 (minutes — the maximum value is 60 hours); the default is 0 (never).
`maxclients`	is the maximum number of clients that can access the server simultaneously; it is therefore the number of sessions with the server. The range and default depend on the User Upgrade Pak installed.

Specifying the Maximum Number of Sessions

You can use the `maxclients` keyword to specify the number of sessions — that is, the number of clients — the server can support at one time. The upper limit is determined by the User Upgrade Pak installed, together with the maximum number of virtual circuits that your transport protocol is configured to support.

To increase the maximum number of sessions, follow these steps:

1. Reconfigure your transport protocol to support a maximum number of virtual circuits greater than or equal to the maximum number of sessions you intend the server to support.
2. Increase the value of the `maxclients` keyword in the server's *lanman.ini* file to a number less than or equal to the number of virtual circuits that you have configured your transport protocol to support.

Note: The maximum allowable value for `maxclients` is 5 for the Base System Package, 10 if the 5-to-10 User Upgrade Pak is installed, 25 if the 10-to-25 User Upgrade Pak is installed, and unlimited if the 75-to-Unlimited User Upgrade Pak is installed.

Viewing Session Information

You can view the following kinds of information about a session with a server:

- the computername and username of each user with a session established
- the kind of networking software (such as LAN Manager) making the connection (the "client type")
- whether or not the user is logged on as *guest*
- how many open files a user has
- how long the session has been inactive

To view session information using the Net Admin Interface, follow these steps:

1. From the `Status` menu, select `Session status.`

   The `Sessions to This Server` dialog box appears.

2. To see more details on an individual session, move the highlight to that session and select the `Zoom` command button.

   The `Session Information` dialog box appears.

3 On Windows clients, select the OK command button.

On MS OS/2 clients, select the Done command button.

The Sessions to This Server dialog box returns.

4 On Windows clients, select the OK command button.

On MS OS/2 clients, select the Done command button.

Equivalent net Command. You can also view session information using the **net session** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Closing a Session

If you need to perform a task at a server that requires you to disconnect one or more sessions — for example, when you need to restore data in a directory — you can close sessions from the server. If the Alerter service is running, the client whose session you are closing is automatically notified.

Closing a user's session does not prevent the user from connecting to a resource. LAN Manager automatically starts a new session the next time the person uses a resource. If a session is inactive when you close it, the user can start a new session without knowing the first session was closed.

To end an individual session, use the Net Admin Interface. To end all sessions at once, use the Command Line Net Interface.

To close a session using the Net Admin Interface, follow these steps:

1 From the `Status` menu, select `Session status.`

  The `Sessions to This Server` dialog box appears.

2 In the list box of sessions, move the highlight to the session you want to close, then select the `Disconnect` command button.

  A request for confirmation appears.

3 To confirm, select the `OK` command button.

  The `Status` menu returns.

4 On Windows clients, select the `OK` command button.

  On MS OS/2 clients, select the `Done` command button.

Equivalent net Command. You can also close one or all sessions using the **net session** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Closing a File

Turning off the server without using the UNIX system **shutdown** command, as well as some kinds of program errors, may leave a file open, and perhaps even locked. You can force a file closed under these circumstances to make it available again.

To close a file using the Net Admin Interface, follow these steps:

1 From the `Status` menu, select `Opened files.`

  The `Opened Files on This Server` dialog box appears.

2 In the list box of open files, move the highlight to the name of the file that you want to close, then select the `Close` command button.

A request for confirmation appears.

3 To confirm, select the `OK` command button.

The `Status` menu returns.

4 On Windows clients, select the `OK` command button.

On MS OS/2 clients, select the `Done` command button.

Equivalent net Command. You can also close a file using the **net file** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Statistics Display

LAN Manager maintains a record of statistics on server and client activity. You can view these statistics to evaluate how often the server is used and how well it is performing. Statistics are cleared each time the server is turned off, and cannot be saved. You can also clear them explicitly.

Server statistics record information about how the server is being accessed. Client statistics record network activity, network errors, volumes of information sent and received, sessions from the client to the server, connections to shared resources, and use of network buffers.

LAN Manager keeps the following statistics:

`Statistics since`	is the date and time the system began keeping this set of statistics (either at the last server startup or the last time the statistics were cleared).
`Bytes received`	is the amount of data the server has received.
`Bytes sent`	is the amount of data the server has transmitted.
`Mean response time (msec)`	is always zero for UNIX system servers.

`Sessions accepted` is the number of times users connected to the server.

`Sessions timed out` is the number of user sessions closed because of inactivity.

`Sessions errored out` is the number of sessions ended because of error.

`Files and pipes accessed` is the number of files and pipes used.

`Comm devices accessed` is always zero for UNIX system servers.

`Print jobs spooled` is the number of print jobs spooled to printer queues on the server.

`Network errors` is the number of data transmission errors.

`System errors` is always zero for UNIX system servers.

`Exhausted buffers:` Windows clients only — lists the number of shortages of big buffers and request buffers.

- `Big buffers`
- `Request buffers`

`Times buffers exhausted` MS OS/2 clients only — lists the number of shortages of big buffers and request buffers.

`Password violations` is the number of incorrect password responses.

`Permission violations`	is the number of user attempts to access resources without the required permissions.

Procedure. To view and clear server statistics using the Net Admin Interface, follow these steps:

1 From the `Status` menu, select `Server statistics.`

The `Server Statistics` dialog box appears.

2 Do *one* of the following:

- To exit without taking further action, go on to Step 3.
- To clear the statistics, follow these steps:

  a Select the `Clear statistics` command button.

  A request for confirmation appears.

  b To confirm, select the `OK` command button.

3 Windows — Select the `OK` command button.

MS OS/2 — Select the `Done` command button.

Equivalent net Command. You can also view or clear server statistics using the **net statistics server** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Stopping and Restarting the Server

This section describes how to stop and restart the Server Program, which you can do through the UNIX System Administrative Interface or with the **net stop** and **net start** commands.

Stopping the Server Program

Stopping the Server Program prevents users from accessing server resources.

Before stopping the Server Program, you should broadcast a message advising users that the server is coming down. To do so, do *one* of the following:

- At the server, type

  ```
  net send \* "message text"
  ```

  and press ↵.

  For more information on the **net send** command, see the *LAN Manager Troubleshooting and Command Reference*.

- At a client, follow these steps using the Net Admin Interface:

  1 From the `Message` menu, select `Send a typed message`.

  The `Send a message` dialog box appears.

2 Select the `All users of this Server` option button.

3 Type a message in the `Message text box.`

Your message should say when the server will be stopped, and it should advise users to stop their current activities and disconnect their links to the server. Give users adequate time to close their files before you proceed. If you stop the server while users are accessing its shared resources, data may be lost.

4 To send the message, select the `OK` command button.

Procedure using the UNIX System Administrative Interface. Wait until all users have stopped accessing the server. Then, to stop the Server Program immediately using the UNIX System Administrative Interface, follow these steps:

Caution Only *one* person should use the UNIX System Administrative Interface at any given time; otherwise, data may be lost.

1 Access the `LAN Manager Server` menu, as described in Chapter 2.

2 Select `Server Status.`

The system displays the `Server Status` frame and a message indicating the server's current operational status, which should be `Started.`

3 Press the [STOP] function key.

A request for confirmation appears, together with a warning that any clients still linked to the server may lose data.

4 To confirm, type **y** and press ↵.

A confirmation message appears.

5 Press the [CONT] function key.

The `LAN Manager Server` menu returns.

When you are ready to resume server operations, restart the server using the procedure in the next section.

Equivalent net Command. If you are a user with administrative privileges, you can also stop the Server Program using the **net stop server** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Note: When you use **net stop server**, if any clients are still linked to the server, a message appears listing them. The server console itself is included in this list.

Procedure using the Net Admin Interface. Wait until all users have stopped accessing the server. Then, to stop the Server Program immediately, follow these steps:

1 From the `Config` menu, select `Control Services`.

The `LAN Manager Services` dialog box appears.

2 In the list box of services, highlight `Server Service` and select the `Stop` command button.

A request for confirmation appears.

3 To confirm, do one of the following:

If you have an Enhanced MS-DOS client, select the `Yes` command button.

If you have an MS OS/2 client, select the `OK` command button.

A confirmation message appears, stating that the Server Service is stopping. When the server has been stopped, the current focus is changed to the local client.

When you are ready to resume server operations, restart the server using the procedure in the section "Restarting the Server Program" later in this chapter.

Equivalent net Command. If you are a user with administrative privileges, you can also stop the Server Program using the **net stop server** command. For more information, see the *LAN Manager Troubleshooting and Command Reference.*

When you use **net stop server**, if any clients are still linked to the server, a message appears listing them. The server console itself is included in this list.

Restarting the Server Program

Restarting the server does not require rebooting the computer.

To restart the Server Program, you must use the UNIX System Administrative Interface at the UNIX system console. Follow these steps:

Caution Only *one* person should use the UNIX System Administrative Interface at any given time; otherwise, data may be lost.

1 Access the `LAN Manager Server` menu, as described in Chapter 2.

2 Select `Server Status.`

The system displays the `Server Status` frame and a message indicating the server's current operational status, which should be `Stopped`.

3 Press the [START] function key.

A confirmation message appears.

4 Press the [CONT] function key.

The `LAN Manager Server` menu returns.

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

Equivalent net Command. You can also restart the Server Program using the **net start server** command. To use this command, you must be logged on as *root* at the UNIX console. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Synchronizing Network Clocks

You can designate a LAN Manager server as the network time server by having it run the Timesource service. The other computers on the network synchronize with the time server, making it possible to synchronize network events. For example, you can use the Timesource service to ensure that a batch program is run at the same time every day on all computers on the network.

The Timesource service runs only on the time server. It does not keep time, but only provides a reference for other computers on the network. The clock must be maintained by some other mechanism, which is typically special hardware and/or software.

If you will be using the Timesource service routinely, change the value of the `lmxtimesource` keyword in the [*lmxserver*] section of the *lanman.ini* file to `yes`. Then the Timesource service will start automatically whenever you start the server.

Viewing Available Servers and Resources

The Server Program allows you to view the computernames of the other servers available for use on the LAN. It also allows you to view the resources shared with the LAN by those servers. This section provides procedures for viewing available servers and shared server resources.

Viewing Servers

You can view servers that are in your domain and that are not hidden. You can also view servers in other domains that are monitored by the client.

Note: You can hide a server by setting `srvhidden=yes` in the server's *lanman.ini* file.

Use the Net Admin Interface to view servers. From the `View` menu, select `Network servers.`

Equivalent net Command. You can also list visible servers from the client or from the UNIX system console using the **net view** command. For more information, see either the *LAN Manager User's Guide for MS-DOS*, the *LAN Manager User's Guide for MS OS/2*, or the *LAN Manager Troubleshooting and Command Reference.*

Viewing Shared Resources

To view shared server resources using the Net Admin Interface, follow these steps:

1 Set the current focus on a selected server, as described in Chapter 2.

2 From the `View` menu, select `Shared resources.`

The `Shared Resources` dialog box appears, with a list box of shared resources on the server. Administrative resources are not displayed unless the `Show hidden shares` check box is marked.

3 Do *one* of the following:

- To close the list box, go on to Step 4.
- To see more information about a shared resource, follow these steps:

  a Move the highlight to the name of the resource and select the `Zoom` command button.

  On Windows clients, the `Shared Resource` dialog box appears, with a list box of users with links to the resource.

  On MS OS/2 clients, the `Information on the Shared Disk` or `Information on the Shared Print Queue` dialog box appears, with a list box of users with links to the resource.

  b After reviewing the list, select the `Cancel` command button.

4 On Windows clients, select the `OK` command button.

On MS OS/2 clients, select the `Done` command button.

Equivalent net Command. You can also view shared server resources using the **net share** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Using the UNIX System Administrative Interface to View Shared Resources

To view shared server resources using the UNIX System Administrative Interface, follow these steps:

Caution Only *one* person should use the UNIX System Administrative Interface at any given time; otherwise, data may be lost.

1. Access the `LAN Manager Server` menu, as described in Chapter 2.
2. Do *one* of the following:
   - To view shared printer queues, follow these steps:
     a. Select `Printer Administration.`

        The `Printer Administration` menu appears.
     b. Select `Administer Printer Queues.` A list of available shared printer queues appears.
     c. Press the CANCEL function key.

- To view shared directories, follow these steps:

  a Select `Show shared directories.` A list of available shared directories appears.

  b Press the CANCEL function key.

3 Press the CANCEL function key.

The `LAN Manager Server` menu returns.

Chapter 8

Sharing Processor Power

Overview

LAN Manager provides two ways to share processing power--by using LAN Manager's Netrun service and by using distributed applications.

With the Netrun service, users can run programs on a server from clients. As an administrator, you decide how to set up the Netrun service, what programs to run with it, and who can use the programs.

Distributed applications are designed to run on a network. In these applications, several computers run programs using a single set of data.

When a user runs a program with the Netrun service, the program runs on the server, but the user works at a client to start the program, to input data, and to specify the location for the program's output.

With the Netrun service, users can take advantage of the considerable memory, disk space, and processing speed of most servers. Users can run large, time-consuming programs on a server, leaving their own clients free for other work.

The Netrun service also provides an efficient way to run programs that use data files kept on the server. When these programs run on the server, data does not have to be transported from server to client as it does when a client runs this type of program.

You can run any executable UNIX system programs with the Netrun service; however, interactive, screen-oriented programs such as the UNIX System Administrative Interface cannot be used with the Netrun service.

Note: Before making a commercial program available for use with Netrun, check the program's licensing agreement. The licensing terms may limit the number of people who can use the program simultaneously or prevent the program's use with the Netrun service.

To implement the Netrun service, you must do the following:

- Create the run path
- Check that the programs are in the appropriate directories
- Share the directory
- Share the server resources required to run the programs
- Start the Netrun service

To specify the programs that users can run on the server, you create a run path. A run path is a list of directories containing programs available for use with the Netrun service. The run path is set with the *runpath* keyword in the [*netrun*] section of the *lanman.ini* file.

Caution Do not depend on the `runpath` keyword to ensure secure operation. The most reliable security control for the Netrun service is the permissions you put on the \*pipe**lanman**netrun* named pipe. See "Controlling Access to Netrun and Distributed Applications" later in this chapter.

If you change the value of *runpath* while the Netrun service is running, you must restart the Netrun service for the change to take effect.

When defining the run path, check that directories in the run path contain only programs that you want users to run. For example, if you put */usr/bin* in the run path, users have full administrative access to the server.

The directories in the run path can reside on any server in the network. They do not have to be shared for the Netrun service to work–in fact, there is a good reason not to share them. If a directory in the run path is shared, a user can add a new program to that directory and run the program on the server. If you share a directory that is in the run path, be sure to limit users' access to the directory when you assign permissions.

The Netrun service on UNIX system servers invokes a Bourne shell to execute the submitted command. The `runpath` is passed as an environment variable. The command can use Bourne shell features such as wildcard expansion and shell commands.

For example, the command `netrun rm -rf /*` will be rejected if the **rm** executable does not appear in one of the directories indicated by the `runpath` keyword, but `netrun exec /usr/bin/rm -rf /*` will succeed.

Controlling Access to Netrun and Distributed Applications

The Netrun service and distributed applications create and use named pipes to send information to the various computers running the program or application. On servers with user-level security, you can assign permissions to these named pipes to control access to the programs. *pipe\lanman\netrun* is the named pipe the Netrun service uses. For the names of the named pipes used by specific distributed applications, see the applications' manuals.

IPC$, an administrative resource that controls how interprocess communication (IPC) works on servers, must be shared for the Netrun service or distributed applications to work. IPC$ is automatically shared on servers with user-level security, but you must explicitly share IPC$ on servers with share-level security. For more information on sharing the IPC$ resource, see the *LAN Manager Troubleshooting and Command Reference.*

All programs running with the Netrun service run as if started at the server by the user lmxguest with adminstrative privileges. As a result, all network file security is bypassed. Local security is based on the UNIX system *uid lmxguest* and *gid lanman.* You should make only carefully designed programs available via the Netrun service to non-administrators. In particular, you should not make any command interpreter (for example */sbin/sh, csh,* or *ksh*) available for use with the Netrun service.

Note: For more control over access rights for the Netrun service, run the server with user-level security.

Controlling Access with User-Level Security

On a server with user-level security, you can restrict access to programs available through the Netrun service and to distributed applications by setting the permissions for the named-pipe resource that these files use (*pipe\lanman\netrun* for the Netrun service). Only users with permissions to use the named pipe can use the Netrun service or the distributed application.

You can assign the following permissions for a named pipe to a user or group:

- Permitted access (Yes)

  User or group can use the named pipe. (Yes includes the Read and Write permissions.)

- Denied access (No)

  User or group cannot use the named pipe.

- Permitted access; can change permissions (Yes + P)

  User or group can use and set access permissions for the named pipe.

You can also set default permissions, which are the permissions assigned for the \pipe resource.

To control access to individual programs, set the permissions for each program file in the run path. Only users who have R or X (Read or Execute) permission for a program can run the program with the Netrun service.

For information on setting permissions for directories and files, see Chapter 3.

Setting Permissions For a Named-Pipe Resource

To set permissions for a named-pipe resource, follow these steps:

1. From the `Accounts` menu, select `Other permissions`.

   The `Select a Queue or Pipe for Access Permissions` dialog box appears.

2. From the `Access type` option buttons, select `Named pipes`.
3. Select the `Add entry` command button.

   The `Add Permissions for Named Pipe` dialog box appears.

4. In the `Sharename` box, type the name of the pipe.
5. Do one of the following:

   - For the Netrun service, type the sharename *lanman\netrun*.
   - For the names of the named pipes used by a specific distributed application, see the manual(s) for that application.

6 Set the permission for the named pipe.

- To grant permissions for a group or a user, in the `No assigned permissions` box, select the groupname or username. From the `Assigned permission` option buttons, select the permission you want to assign for the group or user, and then select the `Permit` command button.

  The groupname or username moves to the `Assigned permissions` box.

- To change the permissions for a group or a user, in the `Assigned permissions` box, select the groupname or username. From the `Assigned permission` option buttons, select the permission you want to assign the group or user.

- To revoke the permissions for a group or a user, in the `Assigned permissions` box, select the groupname or username, and then select the `Revoke` command button.

  The groupname or username moves to the `No assigned permissions` box.

- To reset the permissions for this resource to the default permissions, select the `Use default permissions` check box.

  To set default permissions for all named pipes, see Chapter 3.

- To revoke permissions for all users, select `<Revoke all>`.

7 From the `Enable auditing for` check boxes, select one or both boxes to audit successful or failed attempts to use this resource.

This could be used to provide information on how extensively the resource is used, and whether you need to provide greater access to the resource (perhaps by licensing more users).

8 Select the `OK` command button.

9 On Windows clients, select the `OK` command button.

On MS OS/2 clients, select the `Done` command button.

Viewing or Changing Permissions For a Named-Pipe Resource

You can view or change permissions for a named-pipe resource from the Net Admin Interface for Windows or from the Net Admin Interface for MS OS/2.

Procedure from the Net Admin Interface for Windows. To view or change permissions for a named-pipe resource, follow these steps:

1 From the `Accounts` menu, select `Other permissions`.

The `Other Permissions` dialog box appears.

2 From the `Available/Shared Resources` dialog box, select Pipe.

3 Select the named pipe whose permissions you want to view, and click on it.

The `Users with Permissions` dialog box appears and lists the current users with their permissions.

4 If you wish to change permissions for the named pipe, do the following, as appropriate:

- To grant permissions for a group or a user, in the `Users without permissions` box, select the groupname or username. From the `Assigned permission` option buttons, select the permission you want to assign for the group or user, then select the `Permit` command button.

  The groupname or username moves to the `Users with permissions` box.

- To change the permissions for a group or a user, in the `Users with permissions` box, select the groupname or username. From the `Assigned permission` option buttons, select the permission you want to assign the group or user.

- To revoke the permissions for a group or a user, in the `Users with permissions` box, select the groupname or username, and then select the `Revoke` command button.

  The groupname or username moves to the `Users without permissions` box.

- To reset the permissions for this resource to the default permissions, select the `No default permissions` check box.

- To reset default permissions for all named pipes, see Chapter 3.

- To revoke permissions for all users, select `Revoke all.`

Auditing provides information on how extensively the resource is used, and whether you need to provide greater access to the resource (perhaps by licensing more users).

5 To audit successful or failed attempts to use this resource, do the following:

   a Select the Audit command button.

   b Select and mark the tasks you wish to audit.

6 Select the OK command button.

7 Select the Done command button.

Procedure from the Net Admin Interface for MS OS/2.

1 From the Accounts menu, select Other permissions.

   The Select a Queue or Pipe for Access Permissions dialog box appears.

2 From the Access type option buttons, select Named pipes.

3 Select the named pipe whose permissions you want to view, then select the Zoom command button.

   The Add Permissions for Named Pipe dialog box appears.

4 If you wish to change permissions for the named pipe, do the following, as appropriate:

   - To grant permissions for a group or a user, in the No assigned permissions box, select the groupname or username. From the Assigned permission option buttons, select the permission you want to assign for the group or user, then select the Permit command button.

The groupname or username moves to the Assigned permissions box.

- To change the permissions for a group or a user, in the Assigned permissions box, select the groupname or username. From the Assigned permission option buttons, select the permission you want to assign the group or user.
- To revoke the permissions for a group or a user, in the Assigned permissions box, select the groupname or username, and then select the Revoke command button.

  The groupname or username moves to the No assigned permissions box.
- To reset the permissions for this resource to the default permissions, select the Use default permissions check box.
- To reset default permissions for all named pipes, see Chapter 3.
- To revoke permissions for all users, select <Revoke all>.

5 From the Enable auditing for check boxes, select one or both boxes to audit successful or failed attempts to use this resource.

This auditing could be used to provide information on how extensively the resource is used, and whether you need to provide greater access to the resource (perhaps by licensing more users).

6 Select the OK command button.

7 Select the Done command button.

Controlling Access with Share-Level Security

On a server with share-level security, the IPC$ resource is used to restrict access to programs available through the Netrun services and to distributed applications. You control access to these programs by sharing IPC$ and assigning a password to it. Permissions are granted to those who know the password.

Assigning a password to IPC$ has other effects on security as well. When you assign a password to IPC$, users must explicitly connect to IPC$ and supply the password before they can view the resources shared by the server, use the Netrun service on the server, or run a distributed application on the server. Administrators must type the password before remotely administering the server.

To administer a server with IPC$ shared, from the command line, type a command with the following form:

```
net use \\server\ipc$ password
```

For more information on IPC$, see the *LAN Manager Troubleshooting and Command Reference*.

Controlling the Number of Netrun Users

The optional `maxruns` keyword in the [*netrun*] section of the *lanman.ini* file defines the maximum number of users who can run programs simultaneously on the server using the Netrun service. The range for `maxruns` is 1 through 10 users; the default is 3.

If you change the value of `maxruns` while the Netrun service is running, you must restart the Netrun service for the change to take effect.

Setting Up the Netrun Service

Before starting the Netrun service, you must set up the server so you can start and stop the service. You must have administrative or server operator privileges to stop, pause, or continue this service.

To set up the server for the Netrun service, follow these steps:

1. Change the `runpath` keyword in the [*netrun*] section of the *lanman.ini* file as follows: type the path of each directory containing programs that you want to make available using the Netrun service, separating multiple paths with colons.

   For example, the following `runpath` keyword makes the programs in the *sort* and *db/progs* directories available for use with the Netrun service:

   ```
   runpath=c:/sort:c:/db/progs
   ```

2. If the server has share-level security, share the IPC$ resource.

   IPC$ is automatically shared on a server with user-level security.

   For information on IPC$ and sharing, see the *LAN Manager Troubleshooting and Command Reference.*

3. Share a directory on the server.

   Before using the Netrun service to run a program on a server, the user must connect to a shared directory on the server. You must check that a directory is shared and that users who will use the Netrun service can access the directory.

The directory you share does not have to be in the run path and directories you put in the run path do not have to be shared. You share the directory only so that people using the Netrun service can connect to the appropriate server.

For information on sharing directories, see Chapter 5.

4 Assign permission for the shared resources on the server.

On servers with user-level security, you must ensure that users who will run programs with the Netrun service have permission to use the named pipe *pipe\lanman\netrun*. You must also ensure that each user has R or X (Read or Execute) permission for each program that he or she will be running with the Netrun service.

Starting the Netrun Service

You can start the Netrun service automatically or with the Net Admin Interface. Change options for the Netrun service by editing the *lanman.ini* file.

Note: When you start the Netrun service for the first time and when you add programs to the server's run path, be sure to tell the appropriate users. For security reasons, users cannot use the LAN Manager Screen or any commands to find out which programs are available to them.

Starting Netrun with the Net Admin Interface

To start the Netrun service with the Net Admin Interface, follow these steps:

1 From the `Config` menu, select `Server options`.

The `Set Configuration for Server` dialog box appears.

2 From the `Start server services` check boxes, select `Netrun service`.

3 Select the `OK` command button.

Note: You cannot set the run path using this procedure.

Starting Netrun Automatically

You can specify that the Netrun service start automatically each time the server starts by adding `netrun` to the list of services in the `srvservices` keyword in the [*server*] section of the server's *lanman.ini* file. You must also be sure the run path is set with the *runpath* keyword in the [*netrun*] section of the *lanman.ini* file.

For additional information on the server's *lanman.ini* file, see Appendix B.

Stopping the Netrun Service

Before stopping the Netrun service, check that no one is running a program using the Netrun service. If you stop the Netrun service when a program is running, the program will fail.

To stop the Netrun service, follow these steps:

1. From the `Status` menu, select `Opened files.`

   The `Opened Files on This Server` dialog box appears.

   This dialog box shows which server files are currently in use and who is using them. If *pipe\lanman\netrun* is listed, the user whose name appears by the resource is using the Netrun service to run a program. Wait until this program finishes running before you stop the Netrun service or the program will fail.

2. Select the `Done` command button.

3. From the `Config` menu, select `Server options.`

   The `Set Configuration for Server` dialog box appears.

4. From the `Start server services` check boxes, select `Netrun service.`

5. Select the `OK` command button.

Adding a Program

You can modify the list of programs available under the Netrun service at any time after you begin Netrun.

To add a program for use with the Netrun service, follow these steps:

1 Either move the new program to a directory in the run path or add the directory containing the program to the run path.

If you add a directory to the run path, check that the directory includes only those programs that you want users to access.

To add a directory to the run path, add the path of the directory to the `runpath` keyword in the [*netrun*] section of the *lanman.ini* file. Use colons to separate multiple paths.

2 If the server has user-level security, grant the users who will run the new program either R or X (Read or Execute) permission for the program file.

You may need to adjust UNIX system permissions as well.

3 If you add a directory to the run path, restart the Netrun service so that the changes can take effect.

For instructions on stopping and starting the Netrun service, see "Starting the Netrun Service" and "Stopping the Netrun Service," earlier in this chapter.

Removing a Program

You have three options for removing a program from use with the Netrun service.

To remove a program, use one of these alternatives:

- Move the program to a directory not in the run path.
- Remove the directory containing the program from the run path. Removing the directory prevents all other files in the directory from being used with the Netrun service.

  After you remove a directory from the run path, stop and restart the Netrun service.
- If the server has user-level security, modify a user's permissions for the program. Remove the user's R and X (Read and Execute) permissions to prevent the user from running the program with Netrun.

  You can also modify the UNIX system permissions to remove the "o" permissions for the programs.

Using the Network Application Starter

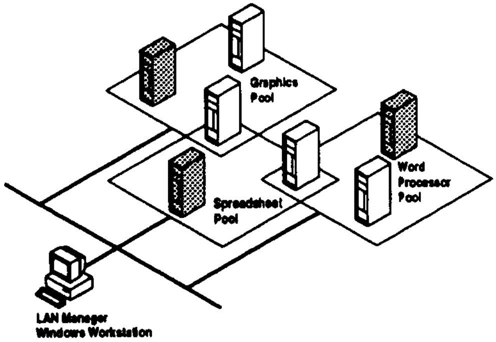
LAN Manager provides a means for you to administer and monitor use of Windows applications (and non-Windows applications that are designed to run with MS-DOS). The Network Application Starter (**appstart**) utility, run on a user's Windows workstation, makes a network connection (**net use**) from the workstation to a remote server, starts up a specified application on that server for the user to run, and deletes the network connection when the user exits the application.

One way to implement **appstart** is to set up a share on a server that contains a particular application, such as a word processor, and limit the number of users to that share to the number of users that your site-license has for the application.

Appstart also provides these features:

- *Application server pools* enable you to set up a pool of servers that can act as viable servers for each application, and **appstart** will select one each time a user tries to use an application. In this way, you can distribute the load.

Figure 8-1: Application Server Pools



- *Centralized logging* enables you to monitor the activity of applications and shares, and track error conditions.
- *Application aliasing* enables you to set up a list of command-line parameters and refer to each with a single name in the icon command line.
- *Centralized appstart.ini files* enable you to use this feature for easier administration of **appstart** installations.

The Appstart Command Line

The command line in the `Program Item Properties` dialog box for the **appstart** utility is of this form:

appstart [*alias* [*parms...*] | [[**/s:~:**\path\to\start] [**/p:#**]
[*drive*:| **UNC**] [\\server]\share\subdir\for\program.exe
[*parm1 parm2 parm3*]]

Command line parameters are defined as follows:

alias [parms...]

The *alias* represents a name of a section in the *appstart.ini* file from which the command line is to be taken. The value for the alias is passed any additional parameters (*parms...*) that come after the alias. See "The *appstart.ini* File" section for more information about using an alias.

/s:~:\path\to\start

The optional **/s:** parameter allows you to specify the starting directory (\path\to\start). If the ~: is used at the front of the directory specification, the network-drive letter selected will be substituted (if the UNC parameter is not specified). If the **/s:** option is not specified, the current Windows directory is used as the default.

For example, **/s:C:\DATA** starts the application in the \DATA directory on the user's C: drive, and **/s:~:\SALES\JAN92\DATA** starts the application in the \SALES\JAN92\DATA directory on the network drive.

Note: If the UNC parameter is specified, no network drive letter will be substituted in the ~: placeholder, and the user's Windows directory is used as the working directory.

/p:#

The optional **/p:** parameter allows you to specify whether the user's path should be changed to include the remote drive or directory. A value of 0 will not change the path; any other value will change the path. Setting this parameter overrides the default value for **ChangePath** in the *appstart.ini* file.

drive:| **UNC**

An optional specification of the drive letter to use, where *drive*: is a drive letter designation. If this value is not specified, **appstart** will select a drive letter that is not in use. If this parameter is **UNC** in all caps, a UNC name will be used and no drive letter will be used.

Note: If you don't specify a drive letter, **appstart** can't change the path for the executable, which may cause some programs to be unable to access their data files or DLLs.

\server

This optional specification, with \\ (double-backslash) on the front of the path, forces **appstart** to use that specific server when connecting. If you don't specify the server on the command line, **appstart** looks in the *appstart.ini* file for information on what server(s) to use.

\share\subdir\for\program.exe

This variable is the complete path to the executable, starting at the share. If you do not specify the \server portion, the *appstart.ini* file is checked for information on which server(s) to use. If the UNC parameter was not specified, a drive letter is assigned to the \server\share portion.

parm1 parm2 parm3

Optional parameters to the application.

The *appstart.ini* File

The *appstart.ini* file is used to set up multiple servers. It is only needed if you want to use the server pool, aliasing, or logging features. The *appstart.ini* file can exist either in the Windows directory of the user's workstation, or in a central location on a server. (For information about centralized *appstart.ini* files, see "Managing a Central *appstart.ini* File.") The *appstart.ini* file follows the format shown in the following example:

```
[servers]
    share1=server1,server2,server3,server4 . . .
    share2=serverA serverB serverC serverD . . .
    wordservers=aserv, bserv, cserv, dserv, eserv...

[options]
    LogFile=\\server\share\path\to\log\logfile.log
    UserMsgVerbose=1
    LogMsgVerbose=1
    LogMultiple=1
    ExitWindows=0
    ChangePath=1

[Windows_Spreadsheet_Program]
    1=\share1\spread\sprdsht.exe
    2=UNC \\server1\winsprd\sprdsht.exe coolspread.dat
    3=/s:z:\data z: \share2\maria\sales\sprdsht.exe
```

Case is not significant in section names.

[servers]

Each line in the optional [servers] section has an entry describing a list of servers that support the named share. Each server should be separated by a comma or a space. There is no limit to the number of shares; however, there is a limit of 1024 bytes for each line of servers. (Theoretically, 1024 bytes is 64 full-length servers per share. In practice, most server names are not that long, so you could have even more.)

[options]

The [options] section is optional and may contain any or all of the following parameters:

LogFile

Provides the local or UNC path to a log file for logging system events. When this parameter is used, each time a user enters an application, the username, machine name, date and time, server selected, and application are logged. The same information is logged when the user exits the application. Any fatal errors are also logged. If the user needs other types of tracking, the LAN Manager auditing feature can be used to audit the actual file usage.

UserMsgVerbose and **LogMsgVerbose**

Allow the administrator to specify how much information is displayed to the user and how much information is sent to the log file when an error occurs, respectively. A value of 1 in either parameter causes **appstart** to display/send all of the information it has. A value of 0 causes **appstart** to display/send a simple message stating that the **appstart** command failed. The default value is 1 (verbose) for both parameters.

LogMultiple

Specifies whether to log multiple instances of the same alias. For example, if the user launches an application twice, without exiting, both instances can be logged. The default is 1 (log multiple instances).

ExitWindows

Specifies whether **appstart** should allow the user to exit Windows without first exiting **appstart**-launched applications. If this value is 1, **appstart** will let the user exit Windows, and it will attempt to clean up any used resources on the exit. If this value is 0, **appstart** will *not* let the user exit until all **appstart**-

started applications have been exited.

Note: The default is to not let the user exit Windows. Under Windows 3.*x*, allowing the user to exit may cause a UAE.

ChangePath

Sets a flag for whether to add the remote drive/directory to the user's path. The default value is 1 (add the remote drive/directory).

Note: A Windows 3.*x* problem sometimes causes the spawned application to UAE with the **ChangePath=1** option. (This problem is fixed in Windows for Workgroups 3.1.) Until the Windows 3.*x* problem is fixed, it is recommended that you set **ChangePath=0.**

[*alias*]

Aliasing is completely optional.

To create an alias for a particular application or use, all you have to do is to create an entry under the name you would like to use, for example, **[Windows_Desktop_Publisher]**. You can use up to 50 characters in the alias. The only restriction is that the alias must be a single word; you cannot use spaces.

Under the alias, you create entries labeled **1=**, **2=**, etc., to signify the first command line to use, the second, etc. The text after the equal sign (=) follows the rules for the command line structure of **appstart**, with the exception that you can't have nested aliases. If you have more than one entry for a particular alias,

appstart will try each one in the numbered order until it is successful or runs out of command lines.

appstart.ini Example

The following example *appstart.ini* file shows how to set up servers, options, application aliases, and a centralized logging file:

```
[servers]
    apps=production,database,mrkting

[options]
    LogFile=\\bigguy\c$\lanman\logs\appstart.log
    UserMsgVerbose=0
    LogMsgVerbose=1
    LogMultiple=1
    ExitWindows=0
    ChangePath=0

[notepad]
    1=\\bigguy\win31$\notepad.exe
    2=UNC \\bigguy\win31$\notepad.exe

[dos_word]
    1=x: \\production\apps\word5.5\word.exe
    2=\apps\dword500a\word.exe
    3=x: \apps\word55\word.exe
    4=/s:~\newsltr \\mrkting\apps\word5.5\word.exe
```

Administering Appstart

Before you set up an application for use with **appstart**, be sure to consider the license implications of making the application available on a server. Some applications require a license for each user, rather than for each installation.

Preparing to Use Appstart

To set up applications for users to run with **appstart**, you must:

- Install the application on a server (or a pool of servers).
- Share the application directories.
- Set permissions for the application directories so that users can access them.

To install an application on a server, follow the installation instructions for that application.

Use the procedures in Chapter 5, "Managing Shared Directories," to share directories and set permissions.

Note: You can set up applications to run user-level or share-level security. The only requirement is that the user be able to read and execute application files.

Managing a Central *appstart.ini*

Appstart can be set up so that there is one common *appstart.ini* file that all users can share. To use this feature, simply make sure that the user's environment variable **appstart.ini** (in *autoexec.bat* is set to the literal path to the *appstart.ini* file. This can be a UNC path. For example:

```
set appstart.ini=\\bigserver\appstart\sub-dept1\appstart.ini
```

Managing User Workstations

It is a relatively easy task to set up user workstations to run **appstart** applications, especially if you have them use a central *appstart.ini* file. The procedure could look something like this:

- Set up Program Items, using aliases, for applications in a group.
- Copy the group to the user's desktop.
- Edit the user's *autoexec.bat* file to point the *appstart.ini* environment variable to the *appstart.ini* file.

Refer to the *Using LAN Manager with Microsoft Windows* guide for information on setting up **appstart** Program Items.

Note: Every **appstart** user will have a local *appstart.ini* file, in the Windows directory on the workstation, even if a central *appstart.ini* file is in use. The local file contains alias sections for each application in use, with **Using***Parm* parameters listed under each. These parameters keep track of which alias selection has been used, so that if multiple instances of an alias are used, they will map to the same device/server/path combination.

Appendix A: Managing Share-Level Security

Understanding Share-Level Security

This appendix describes the Server Program's share-level security mode. It also describes how to set up a server to run share-level security. While user-level security controls access to resources on a per-user basis, share-level security controls access on a per-resource basis.

Note: Neither the Audit Trail (resource auditing) nor logon validation is available on a server running 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 who knows the password can use that resource, within the limits of the resource's access permissions.

Passwords

Under user-level security, a user needs to know only one password to access resources on a server; that password is part of his or her user account. Once the server verifies the password, it does not ask for it again.

Under share-level security, a user may have to supply a different password for each resource. A share-level server does not maintain a user accounts database. You cannot change a resource password without deleting the sharename and re-establishing it with a different password.

In both security modes, users use the same commands to request access to the server.

Access Permissions

Under share-level security, when you share a resource you assign a set of access permissions for that resource. Share-level security applies 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 (A, C, D, R, W, and X) is the same as for user-level security. However, under share-level security, permissions have the following differences:

- 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 from users accessing the same resource with another sharename and password.
- The P access permission, which means *change access permissions* under user-level security, means *administrators only* under share-level security. See the next section for more information on administration and the P access permission.

How Access to Resources Is Controlled

For each resource that you share, you can define a password and a set of access permissions.

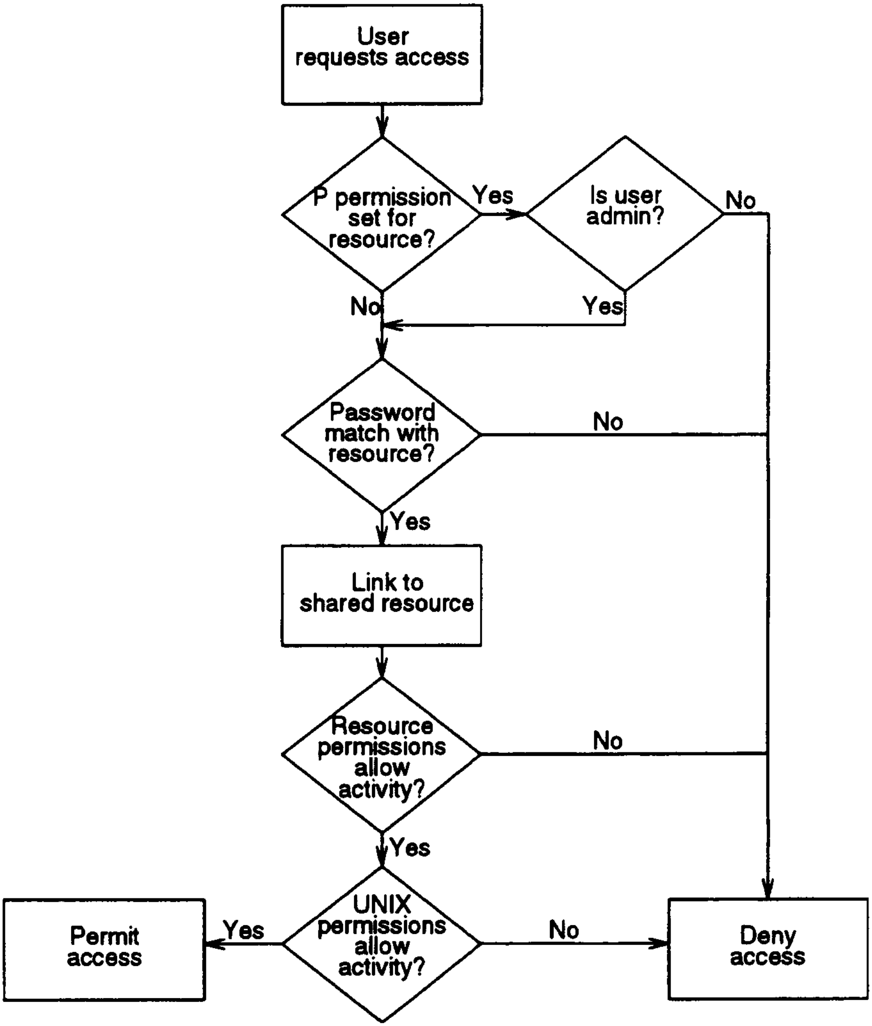
For a user to be able to access the resource, the following conditions must be met:

- 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.

Figure A-1 illustrates how a server running share-level security decides whether a user should be allowed to use a shared resource. This decision depends on the following sequence of checks:

1. Is the P access permission set for this resource? If so, continue to Step 2. If not, continue to Step 3. The P access permission (administrators only, under share-level security) overrides all other access permissions and passwords.
2. Does the user have admin privilege (that is, is the user already linked to the *ADMIN$* resource)? If so, continue to Step 3. If not, deny access.
3. Does the user's password match the resource's? If so, link to the resource and continue to Step 4. If not, prompt once for a different password. If this password does not match, deny access to the resource.
4. Do the share access permissions allow the requested activity? If so, continue to Step 5. If not, deny access.
5. Do the resource's UNIX system permissions allow the requested activity? If so, allow access to the resource. If not, deny access.

Figure A-1: Determining Access to Resources on a Server Running Share-Level Security


User requests access
P permission set for resource?
Yes
Is user admin?
No
No
Yes
Password match with resource?
No
Yes
Link to shared resource
Resource permissions allow activity?
No
Yes
UNIX permissions allow activity?
Yes
Permit access
No
Deny access

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
3. start the Client Program
4. log on as the administrator
5. share directories
6. configure printer ports for printers connected to the server (if necessary)
7. set up shared printer queues

Each of these tasks is described in the following sections.

Planning the Server Setup

To plan share-level security for a server, you must know

- how many users will have access to this server
- what resources (disk and printer) users will 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 specific directory or printer, assign a password to the directory and distribute the password only to users who will be allowed access. To provide access for all users, share the directory and assign no password.

By sharing the same directory under multiple sharenames and passwords, you can also assign different users different access permissions for the same resource.

Configuring the Server

The Server Program runs user-level security by default. To configure your server for share-level security, you must change the value of the `security` keyword in the [*server*] section of the server's *lanman.ini* file.

You can do this by using the UNIX System Administrative Interface to access the `Configure LAN Manager Server` form. In the `Security mode:` field, change the value displayed from `user` to `share.` You must stop and restart the Server service for this change to take effect.

Sharing the Administrative Resources

Under user-level security, an administrator is any user account with admin privilege. Share-level security, on the other hand, does not recognize the concept of user privilege levels. Under share-level security, an administrator is anyone who is linked to the *ADMIN$* resource.

Caution To prevent security breaches, it is important to assign *ADMIN$* a password and to give the password only to users who will administer the server from a client. At installation, the password for the *admin* user is assigned to the *ADMIN$* resource.

Do not assign the P access permission to *ADMIN$*; if you do, you will not be able to link to the resource and you will not be able to administer the server.

To administer a share-level server, you must log on to the network as the user **`admin`** and enter the *ADMIN$* resource password at the `Password:` prompt. The first time you use a **net** command, you are linked automatically to the *ADMIN$* resource.

If you do not use this username and password, you must explicitly link to the server's *ADMIN$* resource before you can perform administrative functions.

To do so, use the **net use** command, as follows:

```
net use x: \\uname.serve\admin$ password
```

Replace *uname* with the server's UNIX system name and *password* with the password for the *ADMIN$* resource.

You can assign the *IPC$* resource a password on a server running share-level security, but it is not recommended that you do so. If you assign *IPC$* a password, users must supply the password to view lists of resources available on the server and to run distributed applications. In addition, to perform remote administration when *IPC$* has a password, administrators must first connect to *ADMIN$*, then supply both the *ADMIN$* and the *IPC$* passwords.

Caution Do not assign a password to the *IPC$* resource.

Procedure. LAN Manager shares the *ADMIN$* and *IPC$* resources automatically. However, if you have unshared one of these resources, you can start sharing it again.

Note: To enable remote administration of a server, the server must share both *ADMIN$* and *IPC$*. To prevent remote administration of a share-level server, you can choose to unshare one or both of these resources. However, if *IPC$* is unshared, users cannot view the server's resources and the Command Line Net Interface commands will not work. To prevent remote administration but allow users to view resources, unshare *ADMIN$* but not *IPC$*.

To share *ADMIN$* or *IPC$* using the Net Admin Interface, follow these steps:

1 From the `View` menu, select `Shared resources.`

  The `Shared Resources` dialog box appears, with a list box showing the server's shared resources.

2 Mark the `Show hidden shares` check box.

3 Select the `Add share` command button.

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

4 Select the `Admin share` option button, then select the `OK` command button.

  The `Add a Reserved Administrative Share` dialog box appears. If the server is running share-level security, there is a `Password` text box in this dialog box.

5 From the `Sharename` option buttons, select `ADMIN$` or `IPC$.`

6 In the `Remark` text box, optionally type a comment.

This comment will be displayed when administrators view the server's shared resources.

If you do not type a comment, LAN Manager displays the default comment: `Remote ADMIN$` or `Remote IPC$`.

7 In the `Password` text box, do *one* of the following:

- If you are sharing *ADMIN$*, type a password.
- If you are sharing *IPC$*, do not type a password.

8 In the `User limit` option buttons, do *one* of the following:

- To set no limit on the number of users who can use the resource simultaneously, select `Unlimited`.
- To set a limit, select `Max. users` and type the number in the adjacent text box.

9 On Windows clients, select the `OK` command button.

On MS OS/2 clients, select the `OK` command button.

The `Shared Resources` dialog box returns.

10 On Windows clients, select the `OK` command button.

On MS OS/2 clients, select the `Done` command button.

Equivalent net Command. You can also share *ADMIN$* or *IPC$* using the **net share** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Managing Shared Directories

This section describes how to share and unshare directories on a server running share-level security.

Sharing a Directory

To share a directory on a server running share-level security using the Net Admin Interface, follow these steps:

1. From the `View` menu, select `Shared resources.`

   The `Shared Resources` dialog box appears.

2. Select the `Add share` command button.

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

3. Select the `Disk directory` option button, then select the `OK` command button.

   The `Share a Directory with the Network` dialog box appears.

4. In the `Sharename` text box, type a name for the resource.

   A sharename must follow MS-DOS file naming conventions. The sharename does not have to be the same as the directory name.

5. Do *one* of the following:

   - Using the `Path` text box, type the complete path (including the drive ID, **c:**) of the directory that you want to share.

Note: The Net Admin Interface for Windows requires that the directory already exists. If the directory does not exist, the Net Admin Interface for MS OS/2 prompts you to create it. Select OK to create it.

- Using the Contents of text box:

  a Select the Dir command button.

  A list box of directories appears.

  b To select a directory and see a list of its contents, move the highlight to the name of the directory.

  On Windows clients, select the Directory command button.

  On MS OS/2 clients, select the Dir command button.

  As you move the highlight, the text in the Contents of text box changes to show the selected directory.

  c To return to the directory one level up, with .. (parent directory) highlighted in the text box, select the Windows Directory or the MS OS/2 Dir command button.

  d Repeat Steps b and c until the Contents of text box contains the name of the directory you want to share.

6 In the Remark text box, optionally type a comment describing the resource. Users will see this comment when they view a list of available resources.

7 In the `Password` text box, optionally type a password of up to eight characters for the directory.

If you leave this text box blank, no password is required for users to access the directory.

8 To specify the number of users allowed to access the directory at one time, from the `User limit` option buttons, select *one* of the following:

- `Unlimited` to set no limit.
- `Max users` to set a limit.

If you select `Max users`, in the adjacent text box, type the maximum number of users allowed. If a number appears in this text box when you select the button, the value is from the `maxclients` keyword in the [*server*] section of the server's *lanman.ini* file. You can type over it with a lower number, but you cannot exceed it. (For information on raising the value of `maxclients`, see Chapter 7.)

9 To set permissions for the directory, in the `Permissions` check boxes, mark the appropriate permissions.

To restrict the directory to users with admin privilege, mark the `Admin only` check box.

10 Select the `OK` command button.

> **Note:** If the directory does not exist, the Net Admin Interface for MS OS/2 prompts you to create it. Select `OK` to confirm creating the directory.

The `Shared Resources` dialog box returns.

11 Windows — Select the `OK` command button.

MS OS/2 — Select the `Done` command button.

Equivalent net Command. You can also share a directory using the **net share** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Unsharing a Directory

To stop sharing a directory using the Net Admin Interface, follow these steps:

1. From the `View` menu, select `Shared resources.`

   The `Shared Resources` dialog box appears.

2. In the list box of shared resources, move the highlight to the directory that you want to unshare, then select the `Stop sharing` command button.

   A request for confirmation appears.

3. To confirm, select the `OK` command button.

   The `Shared Resources` dialog box returns.

4. Windows — Select the `OK` command button.

   MS OS/2 — Select the `Done` command button.

Equivalent net Command. You can also stop sharing a directory using the **net share** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Managing Passwords and Access Permissions

You may need to change a resource password or view or change access permissions under the following circumstances:

- when a user who should have access to a resource cannot 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

For instructions on viewing and changing access permissions, see Chapters 5 and 6.

To change a resource password, you must use the Net Admin Interface to unshare the resource and then share it again, assigning it a new password.

Equivalent net Command. You can also change a resource password using the **net share** command. For more information, see the *LAN Manager Troubleshooting and Command Reference*.

Managing Replication

On a server running share-level security, the export directory tree (*lanman/repl/export*) is automatically shared as *REPL$* with RXA permissions when you start the Replicator service. It is shared without a password.

Appendix B: The Server's lanman.ini File

Overview

This appendix describes the organization of the server's *lanman.ini* file, which is located in the UNIX system directory *lanman*. The contents of this file, a collection of keywords with associated values, define the configuration of the Server Program. When the Server Program is installed, default values are assigned to the keywords in the *lanman.ini* file.

Organization of the File

The *lanman.ini* file is divided into many sections. Each section name appears in the file on a line by itself above the set of keywords contained in that section. Following are the section names:

- [*server*] contains keywords common to all LAN Manager servers.
- [*workstation*] contains keywords that identify the server's domain.
- [*uidrules*] contains keywords that specify the rules governing the mapping of LAN Manager user accounts to UNIX system user IDs.
- [*netlogon*] contains keywords used to configure logon validation.
- [*lmxserver*] contains keywords unique to UNIX system LAN Manager servers.
- [*ups*] contains keywords that specify how the server will react in the event of a power failure.

- [*replicator*] contains keywords that control the Replicator service.
- [*remoteboot*] contains keywords that control the Remoteboot service.
- [*fsi*] contains keywords that identify the server's file system types.
- [*psi*] contains keywords that identify the server's printer subsystems.
- [*services*] contains keywords that specify the services that can be controlled on the server.
- [*version*] contains a keyword that specifies the version of the currently installed LAN Manager server.
- [*netrun*] contains keywords that are used to configure the Netrun service.

Syntax of the File

Within each section, the keywords are listed as follows:

- The name of each keyword is at the beginning of a line, followed by an equal sign and the value assigned to it: *keyword=value*
- Comments start with a semicolon (;). If a semicolon precedes a keyword on the line, that keyword is ignored.
- When a list of values is assigned to a keyword, the values are separated by commas: *keyword=value , value , value* , . . . (There are some exceptions to this rule, which are noted in the description of the appropriate keywords.)

- When a value consists of a path, the path may be absolute, starting with / . If a path does not start with / , it is assumed to be relative to *lanman*.
- If a numeric value begins with 0 it is octal; if it begins with X it is hexadecimal; if it begins with a number from 1 to 9 it is decimal.
- When a keyword has no assigned value (nothing to the right of the equal sign), the value is 0 for a keyword that requires a number and null for a keyword that requires a character string.

  A null value is not valid for all keywords. For example, the `auditing` keyword must have a value of `yes`, `no`, or a list of audited events; a null value prevents the server from starting.

When the Server Program is installed, the *lanman.ini* file contains some default keyword values. Other keywords and the titles of the sections to which they belong are added when you change the Server Program configuration. Only keywords that have been changed to some value other than their default value are added to the *lanman.ini* file. If a keyword does not appear in the file (or is commented out with a semicolon), it is set to its default value.

Changing Keyword Values

To reconfigure the Server Program, you can use one of the following methods to modify the *lanman.ini* file:

1 The UNIX System Administrative Interface. When you change various attributes of the Server Program through this interface, the LAN Manager software changes the appropriate keywords in the *lanman.ini* file.

2 The Net Admin Interface. When you use this interface to administer the Server Program, the appropriate keywords are changed.

The following sections describe the keywords in each section of the *lanman.ini* file.

[server] Section

`accessalert`

The number of resource access violations that can occur before the server sends an alert to the `alertnames` list.

Values: `0 – unlimited`; default: `5`

`alertnames`

A list of the user accounts to receive administrative alerts.

Default: `admin`

`auditing`

Enables or disables auditing, in conjunction with the `noauditing` keyword.

Values: `yes` (enabled), `no` (disabled), or one or more of `logon`, `logonlimit`, `netlogon`, `goodnetlogon`, `badnetlogon`, `permissions`, `resource`, `service`, `sesslogon`, `goodsesslogon`, `badsesslogon`, `use`, `gooduse`, `baduse`, `userlist`; default: `no`

`autodisconnect`

The interval, in minutes, that the server will wait before dropping the virtual circuit to an inactive client.

Values: 0 – 3600 (60 hours); default: 0 (no automatic disconnect)

`erroralert`

The number of errors that can occur before the server sends an alert to the `alertnames` list.

Values: 0 – unlimited; default: 5

`listenname`

The server's name on the network. This keyword takes precedence over the `listenextension` keyword in the [*1mxserver*] section.

Values: any name of 1-15 characters;
default: *name*.**serve**, where *uname* is the server's UNIX system name

`logonalert`

The number of logon violations that can occur before the server sends an alert to the `alertnames` list.

Values: 0 – unlimited; default: 5

`maxauditlog`

The maximum size, in KBytes, of the audit log file on the server.

Values: 0 – unlimited; default: 100

maxclients

The number of clients the server can handle simultaneously, that is, the maximum number of sessions.

Values: The Base System Package is 1 – 5. The User Upgrade Paks are: 5 - 10, 10 - 25; 25 - 75; and 75 - unlimited, where unlimited equals 250. defaults: 5,10,25,75 and 250, respectively.

maxerrlog

The maximum size, in KBytes, of the error log file on the server.

Values: 0 – unlimited; default: 100

noauditing

Disables or enables auditing, in conjunction with the auditing keyword.

Values: yes (disable auditing), no (enable auditing), or one or more of logon, logonlimit, netlogon, goodnetlogon, badnetlogon, permissions, resource, service, sesslogon, goodsesslogon, badsesslogon, use, gooduse, baduse, userlist; default: there is no default `security`

The server's security mode.

Values: `user` (user-level) or `share` (share-level); default: `user`

`srvannounce`

The interval, in seconds, at which the server will announce its presence to the network. This keyword has an effect only if `srvhidden=no`.

Values: `1` – unlimited; default: `180`

`srvcomment`

The descriptive comment that the server sends when it announces its presence to the network.

Values: up to 48 characters; default: `LAN Manager for UNIX Server`

`srvheuristics`

The UNIX system server does not interpret the value of this keyword.

`srvhidden`

Specifies whether the server is hidden on the network. If the server is not hidden, it announces its presence at the interval set by `srvannounce` and can be viewed using the **net view** command.

Values: `yes` (hidden) or `no` (visible); default: `no` `srvservices`

The list of keywords for the services that will start automatically when the server is started. Because services are started in the order they appear in the srvservices entry, you must ensure that netlogon appears before any services that require it (such as Remoteboot).

Default: `alerter,netlogon,replicator`

`userpath`

The UNIX system directory on the server to be used as a default parent directory for home directories for new user accounts.

Values: A path up to a maximum of 256 characters; default: `/home/lanman`

[workstation] Section

`domain`

The name of the domain that includes the server.

Values: any name of up to 20 characters, including letters, numbers, and the following characters:
! # $ % & ( ) - . @ ^ _ ` { } ~

default: *uname*`.dom` for a server in a domain, where *uname* is the server's UNIX system name, or `domain` for a standalone server, and the three character extension `.dom` is optional

`othdomains`

The names of other domains visible to the server.

Values: the names of up to four other domains, separated by commas; default: none

[uidrules] Section

`exclude`

UNIX system user IDs excluded from being added as new LAN Manager user accounts.

Values: a list of numbers or ranges of numbers, for example, `0-100,105-109,117,192`; default: `0-100`

`forceunique`

Create new UNIX system user IDs for all new LAN Manager user accounts on the server.

Values: `yes` (create new user IDs) or `no` (do not create new IDs, that is, re-use existing UNIX system accounts for new LAN Manager users); default: `no`

[netlogon] Section

`deltabufsize` The buffer size, in KBytes, used by a backup domain controller or member server for receiving user accounts database updates (changes) from the primary domain controller.

Values: `1` – unlimited; default: `8`

`logonquery` The interval, in seconds, at which the server checks whether linked clients are still active.

Values: `60` – unlimited; default: `900` (15 minutes)

`maxmember` The number of backup domain controllers and member servers that can receive user accounts database updates from the primary domain controller.

Values: `5` – unlimited; default: `10`

`maxquery` The number of non-responses the server can receive when checking whether a client is still active before removing the client from its list of active clients.

Values: `1` – unlimited; default: `3`

pulse

The interval, in seconds, for sending update notices when no updates are occurring to the master user accounts database. This keyword applies only to a primary domain controller, and is ignored by other servers.

Values: 60 – 3600 (1 hour); default: 300 (5 minutes)

querydelay

The interval, in seconds, that a client can wait before responding to the server's inquiry whether it is still active.

Values: 1 – unlimited; default: 2

randomize

The number of seconds during which a backup domain controller or member server randomizes a request to get updates after receiving an update notice from the primary domain controller. This keyword decreases the odds of servers in the same domain requesting an update from the primary domain controller at the same time.

Values: 5 – 120; default: 30

relogondelay

The interval, in seconds, that a client can wait before logging back on to the server after the server has been stopped and restarted.

Values: 1 – unlimited; default: 2

`scripts`

The location of logon scripts. This keyword applies only to a primary or backup domain controller.

Default on primary controller: `repl/export/scripts`

Default on backup domain controller: `repl/import/scripts`

`ssipasswdage`

The interval, in seconds, at which a backup domain controller or member server must change the password that it sends to the primary domain controller to verify its eligibility to receive user accounts database updates.

Values: `86400` (24 hours) – unlimited; default: `604800` (7 days)

`syncbufsize`

The buffer size, in KBytes, used by a backup domain controller or member server for receiving user accounts database updates from the primary domain controller.

Values: `1` – unlimited; default: `32`

`timediff`

The difference, in seconds, that the primary domain controller will tolerate between its system time and the system time on a backup domain controller or member server when sending user accounts database updates.

Values: `0` (ignore differences altogether) – unlimited; default: `0`

`update`	Controls synchronization of the user accounts database with the master database on the primary domain controller when the server starts. This keyword applies only to a backup domain controller or member server, and is ignored by the primary domain controller. Values: `yes` (synchronize on startup) or `no` (do not synchronize); default: `no`

[lmxserver] Section

Caution Many of the keywords in this section support internal processes or system troubleshooting and debugging. Change any values in this section only under very unusual circumstances and only if you are sure you understand the consequences.

`accessfile`

The location of the file containing the user accounts database.

Values: A path up to a maximum of 256 characters; default: `datafiles/accounts.lmx`

`accessgroup`

The UNIX system group name for the user accounts database file.

Default: `DOS----`

`accesshi`

The value to be assigned to the `accessalert` keyword if `alertthresh=high`. This only applies when you change the value using the UNIX System Administrative Interface. Otherwise, the server uses the values specified by the `accesslert, erroralert,` and `logonalert` keywords.

Values: `0` – `20000`; default: `20000`

`accesslow`

The value to be assigned to the `accessalert` keyword if `alertthresh=low`. This only applies when you change the value using the UNIX System Administrative Interface. Otherwise, the server uses the values specified by the `accessalert`, `erroralert`, and `logonalert` keywords.

Values: `0` – `5`; default: `5`

`accessmed`

The value to be assigned to the `accessalert` keyword if `alertthresh=normal`. This only applies when you change the value using the UNIX System Administrative Interface. Otherwise, the server uses the values specified by the `accessalert`, `erroralert`, and `logonalert` keywords.

Values: `0` – `200`; default: `200`

`accessowner`

The UNIX system user ID for the user accounts database file.

Default: `lanman`

`accessperms`

The UNIX system permissions for the user accounts database file.

Default: `0644`

`admingroupid`

The group ID assigned to the **net admin** \uname.**serve /c** command.

Default: `DOS----`

`adminpath`

The path used to find commands submitted by the **net admin** \uname.serve **/c** command.

Values: A path up to a maximum of 256 characters; default: `bin:/bin:/usr/bin`

`adminuserid`

The user ID assigned to a process executed by the **net admin** \\ *uname*.**serve /c** command.

Default: `lmxadmin`

`alertthresh`

Sets the frequency with which alerts are generated and sent to the `alertnames` list. This keyword controls the values of the `accessalert`, `logonalert`, and `erroralert` keywords. This only applies when you change the value using the UNIX System Administrative Interface. Otherwise, the serve uses the values specified by the `accessalert`, erroralert, and logonalert keywords.

Values: low, normal, or high; default: low

annomailslot

The name of the mail slot used for the periodic server announcements.

Values: A path up to a maximum of 256 characters; default: *\MAILSLOT\LANMAN

Note that backslashes must be doubled on input or else the entire input line must be enclosed in single quotation marks. (Type *text\\text or 'text\text'* to enter text with a single backslash.)

audlogfilename

The location of the audit log file.

Values: A path up to a maximum of 256 characters; default: lanman/logs/net.aud

audloggroup

The UNIX system group ID for the audit log file.

Default: DOS----

audlogowner

The UNIX system user ID for the audit log file.

Default: lanman

`audlogperms`

The UNIX system permissions for the audit log file.

Default: `0664`

`byemessage`

Specifies whether the server will send a message to all clients in the domain if it is going to stop for any reason other than a normal shutdown. The message states that the LMX Lan Manager has stopped.

Values: `yes` (send a message) or `no` (do not send a message); default: `yes`

`checkpoint`

If the Server Program has been specially compiled, it includes probes to help with performance monitoring, and must be linked against an appropriate library to make the probes work. This keyword tells the server whether it should make calls to the UNIX system **perfhook** subroutine for performance monitoring.

Values: `yes` (make calls to **perfhook**) or `no` (do not make calls); default: `no`

`clispooltime`

The interval, in minutes, allowed for a job sent to a shared client printer to complete printing. If the printing has not finished by the end of this time, a warning message is sent to the server administrator.

Values: `0` (no warning message) – unlimited; default: `20`

`clstructs`

The maximum number of different clients that can be monitored by the Activity Monitor.

Values: `0` – unlimited; default: `16`

`controllock`

The location of the lock file used to ensure that only one **lmx.ctrl** process is running at a time.

Values: A path up to a maximum of 256 characters; default: `lanman/.LCK.ctrl`

`coreok`

Specifies whether the server can create a core dump file on disastrous failures.

Values: `yes` (allowed) or `no` (not allowed); default: `no` `country`

The country code for server-generated messages.

Values:

Country	Code	Country	Code
Asia	099	Latin America	003
Australia	061	Netherlands	031
Belgium	032	Norway	047
Canada	002	Portugal	351
Denmark	045	Spain	034
Finland	358	Sweden	046
France	033	Switzerland	041
Germany	049	United Kingdom	044
Italy	039	United States	001
Japan	081		

Default: `001`

`cpipgroup`

The UNIX system group of the control pipe used to contact the **lmx.ctrl** process.

Default: `sys`

`cpipname`

The location of the control pipe used to contact the **lmx.ctrl** process.

Values: A path up to a maximum of 256 characters; default: `lanman/.ctrlpipe`

`cpipowner`

The UNIX system user ID for the control pipe used to contact the **lmx.ctrl** process.

Default: `lmxadmin`

cpipperms

The UNIX system permissions for the control pipe used to contact the **lmx.ctrl** process.

Default: 0660

createhomedir

Specifies whether the server automatically creates a home directory for a new user account.

Values: yes (create a home directory) or no (do not create a home directory); default: yes.

debug

Specifies whether debugging is enabled.

Values: yes (enabled) or no (disabled); default: no

debugdir

The name of the directory for creation of debug output files.

Values: A path up to a maximum of 256 characters; default: none

debugpat

Debug output lines include the name of the source file that generated the output. This keyword can specify a series of regular expression filters for this output. These regular expressions are separated by spaces; expressions that begin with ! exclude the matched filenames.

Default: * (any)

`debugsignal`

Specifies whether **kill –16** toggles the debug state of an **lmx.srv** or **lmx.ctrl** process.

Values: `yes` (toggle debug) or `no` (do not toggle debug); default: `no`

`debugsize`

The maximum size, in KBytes, of the debug files. When a debug file reaches this size, it is automatically truncated.

Default: `1024`

`dirbufsize`

The buffer size, in KBytes, that the server allocates to hold the contents of a directory it is scanning for a client.

Values: `256` – unlimited; default: `1024`

`dirperms`

The UNIX system permissions for newly created directories.

Default: `0775`

`errlogfilename`

The location of the error log file.

Values: A path up to a maximum of 256 characters; default: `lanman/logs/net.err`

`errloggroup`

The UNIX system group ID for the error log file.

Default: `DOS----`

errlogowner

The UNIX system user ID for the error log file.

Default: lanman

errlogperms

The UNIX system permissions for the error log file.

Default: 0664

errorhi

The value to be assigned to the erroralert keyword if alertthresh=high. This only applies when you change the value using the UNIX System Administrative Interface. Otherwise, the server uses the values specified by the accessalert, erroralert and logonalert keywords.

Values: 0 – 20000; default: 20000

errorlow

The value to be assigned to the erroralert keyword if alertthresh=low. This only applies when you change the value using the UNIX System Administrative Interface. Otherwise, the server uses the values specified by the accessalert, erroralert, and logonalert keywords.

Values: 0 – 5; default: 5

`errormed`

The value to be assigned to the `erroralert` keyword if `alertthresh=normal`. This only applies when you change the value using the UNIX System Administrative Interface. Otherwise, the server uses the values specified by the `accessalert`, `erroralert`, and `logonalert` keywords.

Values: `0` – `200`; default: `200`

`fileperms`

The UNIX system permissions for newly created files.

Default: `02664`

`fullpermcheck`

Specifies the method of permission verification checking of a file or directory in the Access Control List.

Values: `yes` (check each parent directory up to root) or `no` (revert to standard ACL checking, that is, parent directory); default: `yes`

`gcbuffer`

The buffer size, in KBytes, allocated for each server process for client files.

Values: `1` – unlimited; default: `100`

`getapipe`

The interval, in seconds, the server will wait for the **lmx.ctrl** process to respond to an attempt to contact it. The value may need to be increased on a very busy system.

Values: `1 – 1000` (slightly less than 17 minutes); default: `10`

`groupadd`

The location of the UNIX system command used to add elements to the **/etc/group** file.

Values: A path up to a maximum of 256 characters; default: `/usr/sbin/groupadd`

`groupdel`

The location of the UNIX system command used to delete elements from the **/etc/group** file.

Values: A path up to a maximum of 256 characters; default: `/usr/sbin/groupdel`

`groupexclude`

The range of UNIX system group IDs (starting from 0) to which LAN Manager user accounts are not mapped.

Default: `100` (that is, 0 – 100).

`grpcachesize`

The size of the cach mapping LAN Manager user accounts to UNIX system group IDs.

Values: `50 – 256`; default: `100`

`grpupdate`

The interval, in seconds, at which the server checks the UNIX system file */etc/group* for changes.

Values: `0` – unlimited; default: `300` (5 minutes)

`hashsize`

The number of buckets for the hash table in shared memory to keep track of the various modes that clients have used to open files and set record locks.

Values: `8` – unlimited (powers of 2); default: `128`

`ignoreunix`

Specifies whether the Server Program ignores (overrides) or observes (respects) UNIX system file and directory permissions.

Values: `yes` (ignore UNIX system permissions) or `no` (observe UNIX system permissions); default: `no`

`ipctries`

The number of **read** system calls after which the Server Program checks to see if other work could be done by the server. There is a lot of interprocess communication (IPC) between server processes. The server uses the **read** system call to receive IPC messages, but **read** does not always return the entire message. This keyword ensures that the server does not keep trying forever to get an IPC message, at the expense of other activities the process could be doing.

Values: `1` – unlimited; default: `5`

`keepadmshares` Specifies whether remote administrators are prevented from removing the *ADMIN$* and *IPC$* shared resources.

Values: `yes` (prevented) or `no` (not prevented); default: `yes`

`listenextension` The extension that the UNIX system Listener program, by default, applies to the *uname* of the server computer. The `listenname` keyword in the [*server*] section takes precedence over this keyword.

Values: 0-13 characters and a null value are acceptable; default: `.serve`

`lmaddonpath` The directory for dynamic libraries bound into the Server Program and called at various times during server execution, as described in the */usr/include/lmx/lmaddon.h* header file. The server looks for these dynamic libraries on startup.

Values: A path up to a maximum of 256 characters;

default: `lanman/addon/lmaddon`

`lmxmsgfile`

The location of the server's message file.

Values: A path up to a maximum of 256 characters; default: `lanman/datafiles/msgfiles/lmx001.msg`

`lmxsrv`

The location of the server message block (SMB) program started by the **lmx.ctrl** process to handle clients.

Values: A path up to a maximum of 256 characters; default: `lanman/bin/lmx.srv`

`logonhi`

The value to be assigned to the `logonalert` keyword if `alertthresh=high`. This only applies when you change the value using the UNIX System Administrative Interface. Otherwise, the server uses the values specified by the `accessalert`, `erroralert`, and `logonalert` keywords.

Values: `0 – 20000`; default: `20000`

`logonlow`

The value to be assigned to the `logonalert` keyword if `alertthresh=low`. This only applies when you change the value using the UNIX System Administrative Interface. Otherwise, the server uses the values specified by the `accessalert`, `erroralert`, and `logonalert` keywords.

Values: `0` – `5`; default: `5`

`logonmed`

The value to be assigned to the `logonalert` keyword if `alertthresh=normal`. This only applies when you change the value using the UNIX System Administrative Interface. Otherwise, the server uses the values specified by the `accessalert`, `erroralert`, and `logonalert` keywords.

Values: `0` – `200`; default: `200`

`lptmpdir`

The location of the spooling directory for temporary files used by the UNIX system's LP subsystem.

Default: `/var/spool/lp/tmp/`*`uname`*, where *uname* is the server's UNIX system name `mailslotgroup`

The UNIX system group ID for mail slots created on the server.

Default: `DOS----`

`mailslotowner`

The UNIX system user ID for mail slots created on the server.

Default: `lanman`

`mailslotperms`

The UNIX system permissions for newly created mail slot file system entries.

Default: `0222`

`maldebug`

Specifies whether the Server Program calls the **mount** system call with debugging arguments to **malloc**, **calloc**, **realloc**, **strdup**, and free calls. The Server Program can be compiled to include debugging capabilities for **malloc**, **calloc**, **realloc**, **strdup**, and free calls. Calling **mount** allows the **truss** tool to be used to watch the activity from another program. In addition to calling **mount**, the server keeps track of most of the calls and prints the results to the debug file in the main loop. The output includes the file name, line number, and the number of times there has been unfreed space from the file/line number combination.

Values: yes (enable debugging) or no (disable debugging); default: no

maldebugmin

The minimum threshold of **malloc** instances above which the debugging option generates output.

Values: 1 – unlimited; default: 2

maxadminoutput

The maximum amount of output, in KBytes, that administrative functions can produce.

Values: 1 – 64; default: 20

maxfilesize

The maximum file size, in KBytes, that a client can create on the server.

Values: 100 – unlimited; default: 20000

maxlocknap

The maximum interval, in seconds, that a server process will wait for a shared memory lock to become available.

Values: 5 – unlimited; default: 300 (5 minutes)

maxmsdepth

The depth in the mail slot directory, in number of subdirectory levels, to which the Server Program descends in deleting obsolete mail slot nodes when new mail slots are created.

Values: 0 – 100; default: 5

`maxmsgsize`

The maximum amount of data, in bytes, that a client can exchange with the server.

Values: `1024` – unlimited; default: `4356`

`maxmux`

The maximum number of outstanding SMBs that any one client can have at a time.

Values: `1` – `10`; default: `3`

`maxopenfiles`

The maximum number of open files that the **setrlimit()** system call can use. UNIX system processes can use **setrlimit()** to adjust the maximum number of files they are prepared to have open simultaneously. The server has an underlying file descriptor multiplexing architecture that takes over if there are no remaining available file descriptors.

Values: `20` – unlimited; default: `1024`

`maxreadsize`

The chunk size, in bytes, for fulfilling large **read** requests from clients. Each **lmx.srv** process handles more than one client at a time. If a client submits a very large read request to the server, the response may take so long that 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 request in chunks and service other clients between chunk reads.

Values: `1` – unlimited; default: `8192`

`maxsvcwait`

Specifies the amount of time (in seconds) the server will wait for a service to respond when it changes the following statuses of the services: pause, continue, install, uninstall.

Values: 5 – unlimited; default: 60

`maxvcperproc`

The maximum number of virtual circuits that each **lmx.srv** process should be able to handle. This limit is normally calculated on the fly by the Server Program, using the `vcdistribution` and `maxclients` keywords. If the value of `maxvcperproc` is non-zero, its value is used instead of the calculated value.

Values: `0 – 50`; default: `0`

`maxwritesize`

The chunk size, in bytes, for fulfilling large **writes** from clients. This keyword provides the same solution to potential problems caused by large **writes** that `maxreadsize` does for large **reads**.

Values: `1` – unlimited; default: `8192`

`memorymap`

Specifies whether the Server Program uses the **mmap** system call to map file data into the server's address space for efficiency. File mapping is attempted only for read-only files.

Values: `yes` (map files) or `no` (do not map files); default: `yes`

`minpassword`

The minimum number of characters for a valid password.

Values: `0` – `14`; default: `6`

`minvcperproc`

The minimum number of virtual circuits that each **lmx.srv** process should be able to handle. This limit is normally calculated on the fly by the Server Program, using the `vcdistribution` and `maxclients` keywords in the [*server*] section. If the value of `minvcperproc` is nonzero, its value is used instead of the calculated value.

Default: `0`

`msdirgroup`

The UNIX system group ID for the mail slots directory.

Default: `DOS----`

`msdirname`

The location of the mail slots directory (relative to *lanman*).

Default: `mailslot`

`msdirowner`

The UNIX system user ID for the mail slots directory.

Default: `lanman`

`msdirperms`

The UNIX system permissions for the mail slots directory.

Default: `0777`

`msgforward`

Specifies whether the LAN Manager software implements message forwarding between clients. Implementation of message forwarding is not recommended.

Values: `yes` (implement forwarding) or `no` (do not implement forwarding); default: `no`

`msgheader`

Specifies whether alerts sent as popup messages include header text. Because headers are likely to be very long and may result in processing difficulties, their inclusion is not recommended.

Values: `yes` (include headers) or `no` (do not include headers); default: `no`

`nativelm`

An additional field in the session setup request/response. This field is generated at run time.

Default: `LAN Manager/x 2.2`

`nativeos`

An additional field in the session setup request/response. This field is generated at run time.

Default: `UNIX (`*release*`) (`*version*`)`, for example `UNIX 4.0 2.1`

`netaddonpath`

The directory where the Server Program looks for dynamic libraries on startup. Dynamic libraries found in the directory are bound into the Server Program and used to access the various network interfaces on the server computer. Sample source for a network interface file is located in the default directory.

Values: A path up to a maximum of 256 characters; default: `lanman/addon /networks`

`nethelpfile`

The location of the help file (relative to *lanman/datafiles/msgfiles*) used by the **net help** command.

Default: `net.hlp`

`nethmsgfile`

The location of the help file (relative to *lanman/datafiles/msgfiles*) used by the **net helpmsg** command.

Default: `neth.msg`

`netmsgwait`

The interval, in seconds, that the server will wait for a response when it sends a message that requires one.

Values: 0 – unlimited; default: 15

`network`

The network device names and NetBIOS name-passing type for the network(s) the server should use.

Values: sets of four items separated by commas, each set of four separated from the next by a space. The following four items are in each set:

1. The device name for virtual circuit access.
2. The device name for datagram network access.
3. A digit identifying the NetBIOS interface convention used by the two devices above. Currently there are two conventions compiled into the server:
   0 = StarGROUP® NetBIOS convention
   1 = Wollengong TCP-IP NetBIOS convention

4 The name of the transport provider, as returned by the **nlsprovider** system call. (For networks not configured to accept incoming connections through the UNIX system Listener program, this can be any arbitrary string.)

Default:
`/dev/starlan,/dev/starlandg,0,starlan,/dev/ntcp,/dev/nudp,1,necp,/dev/nb,/dev/nbdg,2,nb/dev/netbeui,/dev/netbenid,1,netbeui`

`newusershell`

The login shell for new user accounts. The default prevents new users from logging in to the UNIX system using a terminal emulator. To enable login, set this keyword to a real value, such as `/bin/sh`

Default: `/bin/false`

`nfslocks`

Specifies whether the server tries to set UNIX system record locks in files as requested by clients. Record locks may not work on NFS files on a server running NFS. If `unixlocks=no`, this failure will have no effect on the server.

Values: `yes` (set locks) or `no`

(do not set locks); default: `no`

`nonexistusers`

The number of clients in the server's cache of the names of clients that are not on the network. When the Alerter service tries to send a popup message to a client, NetBIOS name resolution can cause unwanted delays if the client is not on the network. To circumvent this problem, the Alerter service caches the names of clients that are not running, and does not send alerts to these clients.

Values: `0` – unlimited; default: `10`

`nosendtime`

The interval, in seconds, that entries are allowed to remain in the server's cache of clients not on the network.

Values: `0` – unlimited; default: `120`

`packageid`

An identifier for the shared memory segment needed by the Server Program.

Values: any single letter; default: `L`

`passmgmt`

The absolute path to the password file management command, used by the server to add users to the UNIX system.

Values: A path up to a

maximum of 256 characters; default: `/usr/bin/passmgmt`

`polltime`

The interval, in seconds, that the server will wait for the arrival of the virtual circuit file descriptor when a new client is connecting to the server through the UNIX system Listener program.

Values: `0` – unlimited; default: `60`

`qnamelen`

Provides dynamic control of the allowable length of the name of a printer queue. LP subsystem commands currently allow class names to be as large as 255 characters, but jobs sent to these classes cannot be controlled and many of the UNIX system commands to manipulate these jobs result in segmentation faults. This keyword is used by printer queue functions to restrict access to queues based on the length of the queuename.

Values: `1 - 255`; default: `14`

`qsched`

The interval, in minutes, at which the Server Program will check whether any printer queues should be started, based on the values of their `start time` parameters.

Values: `1` – unlimited; default: `10`

`queuealloc`

The number printer queue items that should be allocated at a time with the **malloc** system call. For efficiency, items are allocated in batches, not one at a time.

Values: `1` – unlimited; default: `10`

`rdatrend`

The number of sequential file accesses by a client that the Server Program must detect before it begins reading ahead.

Values: `0` (always read ahead) – unlimited; default: `2`

`relmajor`

The major release number of the Server Program.

Default: `2`

`relminor`

The minor release number of the Server Program.

Default: `1`

`remoteboot`

Specifies whether this server runs th Remoteboot service. Values: `yes` or `no`; default: `yes`

`sbstelladmin`

Specifies whether the server is to send an administrative alert message when the maximum allowable number of clients is exceeded.

Values: `yes` (send an alert) or

no (do not send an alert); default: yes

`sbstelluser`

Specifies whether the server is to send a message to the client that tried to link but failed when the maximum allowable number of clients is exceeded.

Values: `yes` (send a message) or `no` (do not send a message); default: `yes`

`schedlogfilename`

The location of the file kept by the server to identify and control the performance of tasks scheduled with the **at** function.

Default: `lanman/datafiles/sched.log`

`sharefile`

The location of the server's share file.

Default: `lanman/sharefile`

`sharegroup`

The UNIX system group ID for the server's share file.

Default: `other`

`shareowner`

The UNIX system user ID for the server's share file.

Default: `lanman`

`shareperms`

The UNIX system permissions for the share file.

Default: `0644`

`sharepipe`

Specifies whether instances of named pipes share the same stream until they are connected to a client. Setting `sharepipe=yes` saves on pipe resources but causes **poll** to return `POLLIN` on all instances of a given named pipe that are in the listening state when a client connection arrives.

Values: `yes` (use the same stream) or `no` (do not use the same stream); default: `no`

`shmgroup`

The UNIX system group ID for the shared memory segment created to allow the various server processes to share the same state.

Default: `sys`

`shmowner`

The UNIX system user ID for the shared memory segment created to allow the various server processes to share the same state.

Default: `lanman`

`shmperms`

The UNIX system permissions of the shared memory segment created to allow the various server processes to share the same state.

Default: `0664`

`spareserver`

Specifies whether the server should try always to have a spare **lmx.srv** process available for another client.

Values: `yes` (start an **lmx.srv** process) or `no` (do not start an **lmx.srv** process); default: `yes`

`sparesrvtime`

The interval, in seconds, that a spare **lmx.srv** process is allowed to run without serving a client before being terminated.

Values: `0` – unlimited; default: `120`

`spipe`

For UNIX System V Release 3.2 systems, the name of the device that can be used to generate Streams pipes.

Default: `/dev/spx`

`srvstathelpfile`

The location of the help file used by the Activity Monitor.

Default: `lanman/fmli/Text.mon`

`stacksize`

The size of the stack, in bytes, for each task internal to the server.

Values: `1000` – unlimited; default: `10000`

`startscript`

The location of the UNIX system shell script (relative to *lanman/bin*) that the **lmx.ctrl** process is to run when the server is started.

Default: lmxstart

stoponcore

Specifies whether the **lmx.ctrl** process is to stop if it finds that an **lmx.srv** process has terminated unexpectedly.

Values: yes (stop) or no (do not stop); Default: no

svcinit

Specifies whether the server is to run the service starter script.

Values: yes (run the script) or no (do not run the script);

Default: yes

svcscript

The name of the script (relative to *lanman/bin*) that starts Server Program services.

Default: lmxsvc

threshold

If the server is specially compiled, this keyword specifies to the internal tasking mechanism how close a stack can come to overflowing before a warning should be generated.

Values: 1 – unlimited; default: 500

unixlocks

Specifies whether record locks created by MS-DOS or MS OS/2 programs are reflected in the UNIX file system.

Values: yes (locks are reflected) or no (locks are not reflected); default: `yes`

`userremark`

The comment string associated with the *USERS* shared resource.

Values: 0 to 48 characters; default `Logon Users Directory`

`ustructs`

The number of structures allocated in shared memory to handle record lock and open file records. The sum of open files and record locks cannot exceed the value of this keyword.

Values: `1` – unlimited; default: `1000`

`uxclosecount`

The number of least recently accessed files that the Server Program closes transparently to avoid reaching the UNIX system's per-process limit. The server uses a technique called file descriptor multiplexing to allow clients to open far more files than the per-process limits would normally allow.

Values: `1` – `20`; default: `5`

`vcdistribution`

Specifies the distribution of clients over **lmx.srv** processes. 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 process should be started. This keyword specifies the distribution of clients over the **lmx.srv** processes.

Values: sets of three integers separated by commas, each set of three separated from the next by a space. In each set, the first number specifies the number of clients; the second is the minimum number of virtual circuits each **lmx.srv** process should support; the third is the maximum number of virtual circuits each process should support.

Default:

```
1,2,4 17,2,5 26,2,6 37,2,7
51,3,10 101,6,20 201,
8,30 1000,10,50
```

Following is the meaning of the default value:

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
50-100	3	10
101-200	6	20
201-999	8	30
1000+	10	50

`waittodrop`

The interval, in seconds, that the **lmx.ctrl** process should wait for a successful response from a **lmx.srv** process after sending a message to drop a link to a client. There can be only one instance of a particular client name being serviced by the server. If the server notices a connection request from a client that is already being serviced, it tries to drop the pre-existing link.

Values: `0` – unlimited; default: `180`

[ups] Section

`poweraddr` The NetBIOS name to which the server sends a message when it receives a SIGPWR signal.

Default: * (all users)

`powermessage` The text of the message to be sent by the server when it receives a SIGPWR signal.

Values: Unlimited characters; default: `The server has suffered a power failure Please contact your administrator for further instructions`

`powertime` The interval, in minutes, at which the server repeats the message sent when it receives a SIGPWR signal.

Values: `0` (send the message one time only) – unlimited; default: `1`

[replicator] Section

You must specify an export path, an import path, or both.

`exportlist`
The list of import servers and domains. When specifying a computername, do not include the two backslashes (\\ ) at the beginning of the name.

Values: a list of 0 – 32 names, separated by semicolons (;); default: none

`exportpath`
The location of the server's export directory tree.

Values: A path up to a maximum of 256 characters; default: `lanman/repl/export`

`guardtime`
The interval, in minutes, that the export directory must be stable (no file changes) before it can be replicated to import servers.

Values: 0 – half the value of `interval`; default: 2

`importlist`
The list of export servers and domains that will replicate files to the import server. When specifying a computername, do not include the two backslashes (\\ ) at the beginning of the name.

Values: a list of 0 – 32 names, separated by semicolons (;); default: none

`importpath`

The location of the import directory tree.

Values: A path up to a maximum of 256 characters; default: `lanman/repl/import`

`interval`

The interval, in minutes, at which the Replicator service checks the export directory for changes.

Values: `1` – `60`; default: `30`

`logon`

Sets the user name that the import server uses to connect to the export server when no user name is logged on at the import server.

Default: guest

`password`

Sets the password name that the import server uses to connect to the export server when no user name is logged on at the import server.

Default: a null password

`pulse`

How often the export server sends update messages to an import server when no change occurs. This value represents multiples of the value of `interval`.

Values: `1` – `10`; default: 3

random

The maximum interval, in seconds, that import servers can wait before accepting file updates. Each server in the domain should have a different value set to avoid simultaneous updates.

Values: 1 – 120; default: 60

repl_dirgroup

The UNIX system group ID for replicated directories.

Default: DOS----

repl_dirowner

The UNIX system user ID for replicated directories.

Default: lmxguest

repl_dirperms

The UNIX system permissions for replicated directories.

Default: 0775

repl_filegroup

The UNIX system group ID for replicated files.

Default: DOS----

repl_fileowner

The UNIX system user ID for replicated files.

Default: lmxguest

repl_fileperms

The UNIX system permissions for replicated files.

Default: 02664

replicate

Specifies whether the server will import files and directories, export files and directories, or do both importing and exporting.

Values: import, export, or both; default: none `tryuser`

Determines whether the import server should try to update directories when a user name is logged on locally.

Values: yes or no; default: no

[remoteboot] Section

For information on keywords in the [*remoteboot*] section, see the *Remoteboot Guide.*

[fsi] Section

Caution Many of the keywords in this section support internal processes or system troubleshooting and debugging. Change any values in this section only under very unusual circumstances and only if you are sure you understand the consequences.

`closeinodecnt` The number of files to close on up to 4 iterative attempts when the system runs out of available inodes.

Values: Up to 4 integers, separated by commas; default: `5,25,50,100`

`fsaddonpath` The location of dynamic link libraries that support file systems on the server.

Values: A path up to a maximum of 256 characters; default: `lanman/addon/fsaddon`

`fslibname` The subdirectory of the directory identified by `fslibpath` where new file systems are located.

Values: A path up to a maximum of 256 characters; default: `lmfsiops.so`

`fslibpath` The location of new file systems on the server.

Values: A path up to a maximum of 256 characters; default: `/usr/lib/fs` `fsmap`

File system type identifiers that map unknown file systems to known file system types.

Values: a comma-separated list of mappings; default: `unknown:s5,nfs:ufs`

`fsnosupport`

Maps an unknown file system to a specified file system.

Default: s5

`maxfstypes`

The total number of file system types (both actual and mapped by the `fsmap` keyword) that can be recognized by the server.

Values: `1` – unlimited; default: `10`

`nfsroot`

Controls whose username and permissions are used when creating files on an nfs mounted directory.

Values: yes (use the server's root account), no (use the client's username); default: no

`remotemounts`

The names of file system types that indicate remotely mounted file systems.

Default: `rfs,nfs`

[psi] Section

`maxspoolers` The maximum number of simultaneous spoolers the server will support. This number must at least equal the number of libraries in `psaddonpath`.

Default: `1`

`psaddonpath` The location of dynamic link libraries that support printer subsystems on the server.

Values: A path up to a maximum of 256 characters; default: `lanman/addon/psaddon`

[services] Section

`alerter`

The name of the Alerter service that will be invoked.

Default `lmx.dmn`

`netlogon`

The name of the Netlogon service that will be invoked. To avoid maintaining a logon table for the **net who** command, which can cause a heavy broadcast load on the network, add **`/netwho:no`** to this keyword value.

Default: `lmx.dmn`

`netrun`

The name of the Netrun service that will be invoked.

Default: lmx.netrun

`nvalert`

The name of the NetView® Alerter program that will be invoked.

Default: `lmx.nvalert`

`remoteboot`

The name of the Remoteboot service that will be invoked.

Default `lmx.rpl`

`replicator`

The name of the Replicator service that will be invoked.

Default: `lmx.repl`

`server`

The name of the main server that will be executed on startup.

Default: `lmx.ctrl`

snmp

The name of the SNMP program that will be invoked.

Default: none

timesource

The name of the time source program that will be invoked.

Default: lmx.ctrl

ups

The name of the Uninterruptable Power Supply program that will be invoked.

Default: none

[version] Section

`lan_manager`	The numeric value of this server's software release. Default: `2.2`

[netrun] Section

`maxruns`

Sets the maximum number of netrun requests that can run simultaneously. The value of this entry affects the `numreqbuf` keyword in the [*server*] section. `numreqbuf` must be at least five times greater than `maxruns`. This keyword is optional.

Values: 1—10 netrun requests; default: 3 netrun requests.

`runpath`

Sets the path where programs for the Netrun service are located. Only programs located in a `runpath` can be executed from a client or another server. Separate multiple path entires with semicolons (;).

Values: A path up to a maximum of 256 characters; default: a null runpath

Chapter C

Appendix C: The Client's lanman.ini File

Overview

This appendix describes the organization of the client's *lanman.ini* file. The contents of this file, a collection of keywords with associated values, define the configuration of the Client Program. When the Client Program is installed, default values are assigned to the keywords in the *lanman.ini* file.

The location of the *lanman.ini* file depends on the type of client:

- On an Enhanced MS-DOS client, *lanman.ini* is located in the \lanman.dos directory.
- On a Basic MS-DOS client, *lanman.ini* is located in the \lanman.dos\basic directory.
- On an MS OS/2 client, *lanman.ini* is located in the \lanman directory.

Because the Client Program expects to find the *lanman.ini* file in these locations, you should never move *lanman.ini* to another directory.

Organization of the File

On an Enhanced MS-DOS or MS OS/2 client, the *lanman.ini* file is divided into sections.

Each section name appears in the file on a line by itself above the set of keywords contained in that section. (On a Basic MS-DOS client, *lanman.ini* has a different structure, described in the section "The lanman.ini File on a Basic MS-DOS Client" later in this appendix.) Following are the section names:

- [*networks*] specifies which LANs the client is able to use. This section is on all clients.
- [*workstation*] specifies the default configuration values for the principle components of the Client Program. This section is on all clients.
- [*messenger*] specifies the default configuration of the Messenger service. This section is on all clients.
- [*netshell*] configures the way the client uses the Net Admin Interface display. It lists usernames and the rate for refreshing the screen. This section is on all clients.
- [*loadopts*] sets how services are loaded into memory blocks. This section is on Enhanced MS-DOS clients only.
- [*node*] specifies the default configuration values for the Node service of the Microsoft TCP/IP Extensions for LAN Manager. Since the Node service requires at least one LAN Manager 2.2 server running the MS OS/2 operating system, refer to the MS OS/2 server documentation for additional information. This section is only on MS OS/2 clients interacting with MS OS/2 servers.
- [*services*] identifies the locations of directories and files used by LAN Manager services. If the value of a keyword in this section does not start with a backslash (\ ), it is assumed to be relative to the *\lanman.dos* directory on an Enhanced MS-DOS or Basic MS-DOS client, or the *\lanman* directory on an MS OS/2 client. This section is on all clients.
- [*version*] identifies the version of LAN Manager. This section is on Enhanced MS-DOS and MS OS/2 clients.

Syntax of the File

On an Enhanced MS-DOS or MS OS/2 client, within each section, the keywords are listed as follows:

- The name of each keyword is at the beginning of a line, followed by an equal sign and the value assigned to it: *keyword=value*
- Comments start with a semicolon (;). If a semicolon precedes a keyword on the line, that keyword is ignored.
- When a list of values is assigned to a keyword, the values are separated by commas: *keyword=value*, *value*, *value*, . . . (There are some exceptions to this rule, which are noted in the description of the appropriate keywords.)
- When a value consists of a path, the path may be absolute, starting with \. If a path does not start with \, it is assumed to be relative to the *\lanman.dos* directory on an Enhanced MS-DOS or Basic MS-DOS client, or to the *\lanman* directory on an MS OS/2 client.
- If a numeric value begins with 0 it is octal; if it begins with X it is hexadecimal; if it begins with a number from 1 to 9 it is decimal.
- When a keyword has no assigned value (nothing to the right of the equal sign), the value is 0 for a keyword that requires a number and null for a keyword that requires a character string.

The lanman.ini File on a Basic MS-DOS Client

Although the *lanman.ini* files for Enhanced MS-DOS and MS OS/2 clients set a number of parameters, the *lanman.ini* file for Basic MS-DOS clients is much simpler. The Basic MS-DOS file consists of command scripts used by *net.exe* to implement the **net** commands.

The file contains a number of entries of the following form:

```
<command pattern>
      <command script>
```

For example, the first entry is

```
help use
use help
      command.com /c type $Puse.hlp
```

When you issue a command that begins with the word **net**, the words that follow are compared with the command pattern. If the contents of the command line match the command pattern, the command script is executed. For example, if you type **net help use** or **net use help**, *net.exe* will use *command.com* to type the file *use.hlp* (which is in the directory *lanman.dos\basic*) to your screen.

If the contents of the command line do not match the pattern, the next pattern in the file is tried. This process is repeated until all patterns have been tried.

There can be more than one command pattern for each script.

The script consists of a list of files, with arguments, that will be executed by the operating system. Script lines can be distinguished from command patterns by the beginnings of their lines. Script lines begin with one or more blanks or tabs.

The script lines can include the switches for command-line options. If the command you type specifies a different value for an option, the value you supply will be used. You can use any order of switches in the command line.

Because the switches specified in this file correspond to keywords in the *lanman.ini* file on an Enhanced MS-DOS or MS OS/2 client, they are listed in the appropriate section of this appendix as if they were keywords. For example, the **net start workstation /himem** switch corresponds to the himem keyword in the [*workstation*] section.

Changing Keyword Values

You can change the keyword values in *lanman.ini* to customize the client's performance. However, it is best to start with the default *lanman.ini* file that is created during installation of the Client Program. If you encounter performance problems or find the client running out of memory, you may need to change the *lanman.ini* file to readjust the client's use of buffers and processes. However, there is a tradeoff between operating speed and amount of memory used: faster operation requires more and larger buffers, but buffers and processes require more memory.

To reconfigure the Client Program, you must edit the *lanman.ini* file directly, using a text editor of your choice.

Except where noted, you must stop and restart the affected service for changes to the *lanman.ini* file to take effect. For the following optional two keywords in the [*workstation*] section, you must reboot the computer:

- `maxcmds`
- `maxthreads`

Note: You can temporarily override some keywords in the *lanman.ini* file by using the **net start wksta** and **net config wksta** commands at the system prompt. Further information is provided in the section "Overriding Keyword Values" later in this appendix.

Why You Change Values

Consider values for entries in the default *lanman.ini* file to be in the following three categories:

- **Values you should change** — For both MS-DOS and MS OS/2 clients, you must supply a value for the client's name, `computername` in the [*workstation*] section. For MS OS/2 clients only, you must supply a value for the network device driver, `net1` in the [*networks*] section. In addition for MS OS/2 clients, you must supply the location of the Workstation service software *(lanman\services\wksta.exe).*
- **Values you want to change** — An example of a keyword you might want to change is `username` in the [*netshell*] section. This is the default name used when a user logs on to the network. You might also want to change values for keywords that require a path.
- **Values you rarely or never change** — The heuristics keywords determine how information is sent and received over the network. The `wrkheuristics` keyword is in the [*workstation*] section. The values for these heuristics keywords are numbers that control aspects of performance, data transfer, and

protocols. The default values are optimum, and typically should not be modified because they work on most types of network hardware. If you encounter a performance problem, you can change these values. For example, you do not want read-ahead on a 300-baud network line because if the data is not actually used, you sacrifice performance. The default value is set to do read-ahead.

Overriding Keyword Values

Some of the keyword values set in the *lanman.ini* file can be temporarily overridden, using options to the **net start wksta** and **net config wksta** commands. When you override a keyword, the value that you specify is effective only for as long as the affected LAN Manager service is running. You have not changed the value in the *lanman.ini* file.

For example, to temporarily increase the size of the message service buffer on an MS OS/2 client to receive longer messages, type

```
net start messenger /sizmessbuf:n
```

and press ↵. Replace *n* with the new size of the message buffer, in bytes.

For information on the **net start wksta** and **net config wksta** commands, see either *LAN Manager User's Guide for MS-DOS* or *LAN Manager User's Guide for MS OS/2*.

The keywords in each section of the *lanman.ini* file are described later in this chapter.

Calculating Memory Usage for an Enhanced MS-DOS Client

All of the buffers that are controlled by the *lanman.ini* file must fit in one 64 KByte memory segment.

When you set values for an Enhanced MS-DOS client, you must ensure that the following formula is satisfied:

```
((numresources*103) + (numservers*68) +
(maxcommands*67) + (numwrkbuf*60) +
(lastdrive*90) + (numwrkbuf*(sizworkbuf+87)) +
(numcharbuf*(sizcharbuf+87)*2) +
(numbigbuf*(sizbigbuf=87)) + ((files+fcbs)*40) +
(numservices*(sizserviceinfo2+4))+18KBytes)

< 64 KBytes
```

[networks] Section

This section is on all clients. If a keyword applies only to specific client types (Enhanced MS-DOS, Basic MS-DOS, or MS OS/2), this is stated in the keyword's description.

`net`*n*

MS OS/2 clients only — the name of the network device driver and the number of the network interface board that the computer uses for its interface to the network. If you change or add a protocol or NetBIOS device driver for a client, you must also change the entries in the *config.sys* file to include the filename of the new driver. If there is more than one network interface board installed in the computer, include one `net`*n* line for each board, where *n* identifies the number of the network. (Typically, a client is connected to one network, so this number is usually the default, `1`.)

Values:
driver`$`**,** *ln* **,** *type* **,** *sess* **,** *ncb* **,** *name* **,**
where

driver
is the filename of the protocol or NetBIOS device driver in the *lanman\drivers* directory. Do not

include the filename extension.

ln
identifies the LAN adapter (LANA), or network interface board number. If the driver is set up to handle more than one of the same kind of network interface board, *ln* specifies which board to access.

type
specifies the driver type. The valid values are `LM10` (LAN Manager driver) and `NB30` (IBM® NetBIOS 3.0 driver).

sess
specifies the number of sessions.

ncb
specifies the number of network control blocks (NCBs).

name
specifies the number of names.

Default:
`netbeui$,0,LM10,`*x*`,`*y*`,`*z*`,` where *x*, *y*, and *z* are the current settings for the transport driver, NetBEUI

`netservices`

Enhanced MS-DOS clients only — specifies the programs necessary to install the interfaces used by NetBIOS applications.

Values: `chknet` (checks to see that the network has been installed), and `minses` (provides the interface between LAN Manager and NetBIOS); default: `chknet,minses`

[workstation] Section

This section is on all clients. The only keyword that must appear in the [*workstation*] section is `computername`. The other keywords are optional.

If a keyword applies only to specific client types (Enhanced MS-DOS, Basic MS-DOS, or MS OS/2), this is stated in the keyword's description.

`cb`

Basic MS-DOS clients only — identical to the 16th character of the `wrkheuristics` keyword for an Enhanced MS-DOS client. Controls compatability mode buffering. Add this `/cb:x` option to the `redir` line in the Basic MS-DOS *lanman.ini* file.

Values: `0` (do not use a buffer), `1` (use a buffer only if there are no outstanding locks on the file), `2` (always use a buffer); default: `2`

`charcount`

Enhanced MS-DOS and MS OS/2 clients only — the number of characters, in bytes, that this client will store before sending them to a pipe or comm queue. Increase this number if you need to limit traffic on the network. You can change this value at any time with immediate effect.

Values: 0 – 65535; default: 16

Valid minimum and maximum values depend on the communication device.

UNIX system servers do not support communication device queues.

chartime

Enhanced MS-DOS and MS OS/2 clients only — the interval, in milliseconds, during which this client will collect data to send to a pipe or comm queue before sending it. Increase this number if you need to limit traffic on the network or if print jobs are being fragmented. You can change this value at any time with immediate effect.

Values: -1 (ignore this keyword and send characters as soon as the charcount buffer is full) – 65535000 (slightly over 18 hours); default: 3000

Valid minimum and maximum values depend on the communication device.

UNIX system servers do not support communication device queues.

`charwait`

Enhanced MS-DOS and MS OS/2 clients only — the interval, in seconds, that this client will wait for a requested pipe or shared communication device that is busy to become available. Increase this number if there is heavy traffic on the network or heavy use of pipes or shared comm devices, and you are willing to wait for pipes. You can change this keyword at any time with immediate effect.

Values: `0 – 65535` (slightly over 18 hours); default: `128` on an Enhanced MS-DOS client, `3600` on an MS OS/2 client

Valid minimum and maximum values depend on the communication device. UNIX system servers do not support communication device queues.

`computername`

This client's name, which must be unique on the network. If the computername matches any other name (computername, username, or domain name) currently in use, the Client Program will not load successfully; when you start the Client Program you will be prompted to change the name. A computername can be up to 15 characters long, and can include letters, numbers, and the following characters: ! # $ % & ( ) - . @ ^ _ ` { } ~ Lowercase letters are converted to uppercase letters.

You may assign a computername that requires a blank character to be compatible with other types of networks. For example:

```
computername = financial 2
```

When you refer to a computername that includes blanks in a LAN Manager command, you must enclose the computername in quotation marks (" "). For example, to assign the computer *financial* 2 using the **net start workstation** command, type the following: **`net start workstation /computer: "financial 2"`**

On a Basic MS-DOS client, the `computername` keyword is a required parameter for the **net start workstation** command.

Default: the client's computername

`domain`

Enhanced MS-DOS and MS OS/2 clients only — The name of the client's domain. This keyword controls which servers and server resources are visible at the client, and where broadcast messages are sent. The value cannot be the same as any computername on the network. A domain name can be up to 15 characters long, and can include letters, numbers, and the following characters:
! # $ % & ( ) - . @ ^ _ ` { } ~

Default: `DOMAIN`

`himem`

Enhanced MS-DOS and Basic MS-DOS clients only, with an 80286 or 80386 CPU and more than 1 MByte of RAM — specifies whether to load a portion of the redirector into the High Memory area (HMA). If you choose to do so, *config.sys* must include an extended memory manager such as *himem.sys* For more information, see the *LAN Manager Installation and Configuration Guide*.

For Basic MS-DOS clients, add the `/himem` option to the `redir` line in the Basic MS-DOS *lanman.ini* file. There is no `yes` or `no` value for Basic MS-DOS.

Values: `yes` (load the redirector), `no` (do not load the redirector), or `optional;` default: no

`keepconn`

Enhanced MS-DOS and MS OS/2 clients only — The interval, in seconds, that this client will maintain an inactive connection to a shared resource.

Values: `1 – 65535` (slightly over 18 hours); default: `600`

`keepsearch`

Enhanced MS-DOS and MS OS/2 clients only — the interval, in seconds, that this client will maintain an inactive file search request.

Values: `1 – 65535` (slightly over 18 hours); default: `600`

`lanroot`

Enhanced MS-DOS clients only — the location of the directory containing this client's *lanman.ini* file.

Default: `c:\lanman.dos`

`lim`

Enhanced MS-DOS clients only — specifies whether to load a portion of the redirector in expanded memory. (The client's *config.sys* file must also include an entry for the expanded memory driver.)

Values: `yes` (use expanded memory; the computer must have LIM Version 4.0 or higher installed) or `no` (do not use expanded memory); default: `yes`

`maxcmds`

Enhanced MS-DOS and MS OS/2 clients only — The maximum number of NetBIOS commands the Client Program can send to all of this client's network adapters simultaneously. Increase this number if you have multiple applications using LAN Manager simultaneously. Command processing takes up memory, so do not specify a higher number than you need. The recommended value is 1.6 × value of `maxthreads`. If you change the value of this keyword, you must reboot the computer to make the change effective.

Values: 5 × (the number of networks in the `wrknets` keyword) through `255`; default: `11` on an MS-DOS client, `16` on an MS OS/2 client.

`maxerrorlog`

MS OS/2 clients only — the maximum size, in KBytes, of this client's error log. This keyword keeps the error log from filling up the hard disk. Reduce the value if you need disk space more than you need extensive error information. You can change this keyword at any time with immediate effect.

Values: `2` – the size of the hard disk; default: `100`

`maxthreads`

MS OS/2 clients only — The maximum number of execution threads that can use the network by means of the Client Program. Increase this number if you have multiple applications using LAN Manager simultaneously. Each thread takes up memory, so do not allocate more than you need. If you change this keyword, you must reboot the computer to make the change effective.

Values: `10` – `254`; default: `10`

`maxwrkcache`

MS OS/2 clients only — the size limit, in KBytes, of this client's large-transfer buffers. Increase this number if the client is used for file-intensive projects, such as copying large files, and better performance is needed.

Values (in multiples of 64): `0` – `640`; default: `64`

`numalerts`

MS OS/2 clients only — the number of program tasks that can be waiting on an alert condition. Increase this number from the default only if this client uses a server-based application whose accompanying documentation directs you to do so. A larger table takes up memory, so do not allocate more space than you need.

Values: `3 - 200`; default: `12`

`numbigbuf`

Enhanced MS-DOS clients only — the number of big buffers that the client uses to receive large files or amounts of data from servers. Buffer size is set with the `sizbigbuf` keyword.

Values: `1 - 255`; default: `1`

`numcharbuf`

Enhanced MS-DOS and MS OS/2 clients only — The number of pipe and communication device buffers. UNIX system servers do not support communication device queues. Increase this number if you are using several pipes or shared comm devices, or you need to transmit large amounts of data across the network to such devices. Each buffer takes up memory, so do not allocate more than you need.

Values: `0 - 15`; default: `2` on an MS-DOS client, `10` on an

MS OS/2 client

numdgrambuf

Enhanced MS-DOS and MS OS/2 clients only — The number of buffers that process incoming datagrams. (Servers use datagrams to broadcast their presence. Datagrams are also used for domain-wide broadcasts.) If this client views domains with many servers, it may need more datagram buffers than the default to handle incoming announcements.

For MS-DOS clients, the value of this keyword is the total number of buffers for all networks listed in the wrknets keyword. For each domain added to the othdomains keyword, increase this value by 1.

For MS OS/2 clients, the value of this keyword is the number of buffers per network listed in the wrknets keyword.

Values: 3 – 112 on an MS-DOS client, 8 – 112 on an MS OS/2 client; default: 3 on an MS-DOS client, 14 on an MS OS/2 client `nummailslots`

Enhanced MS-DOS clients only — the number of mail slots to use locally. You may need to increase this keyword from the default if your network applications require additional mail slots.

Values: `0 – 255`; default: `2`

`numresources`

Enhanced MS-DOS clients only — the maximum number of simultaneous links that this client can establish to shared resources. Do not assign a greater number of client links than is necessary for the client to perform its normal functions.

Values: `1 – 255`; default: `9`

`numservers`

Enhanced MS-DOS clients only — the maximum number of servers to which the client can have active connections.

Values: `1 – 255`; default: `9`

`numservices`

Enhanced MS-DOS and MS OS/2 clients only — The size of the internal service table. Increase this number if this client will be running many LAN Manager services. A larger table takes up memory, so do not allocate more space than you need. The names of the available services are kept in the [*services*] section of the *lanman.ini* file. The value of this keyword should be greater than or equal to the number of keywords in the [*services*] section.

Values: 1 – 255 for an MS-DOS client, 4 – 256 for an MS OS/2 client; default: 5 for an MS-DOS client, 16 for an MS OS/2 client

numviewedservers

Enhanced MS-DOS clients only — the maximum number of servers that can be displayed using the **net view** command and in certain list boxes in the Net Admin Interface for Windows or LAN Manager screen.

Values: 0 – 255; default: 50

numworkbuf

Enhanced MS-DOS and MS OS/2 clients only — The number of buffers this client can use to store data for transmission, thereby increasing efficiency. Each buffer takes up memory, so do not allocate more than you need.

Values: 4 – 50; default: 5 on an MS-DOS client, 15 on an MS OS/2 client

othdomains

Enhanced and MS OS/2 clients only — the names of additional domains visible to this client. The client also receives messages and alerts sent to these domains.

Values: the names of up to four other domains, separated by commas; default: none.

`printbuftime`

MS OS/2 clients only — the interval, in seconds, that the *prn:* print device is kept open for compatibility-mode printer requests. Most applications that work in the MS OS/2 compatibility mode do not explicitly close the *prn:* print device to tell MS OS/2 to send the contents of the printer buffer to the printer queue. This keyword limits how long the *prn:* device will be kept open. You can change this keyword at any time with immediate effect.

Values: `0 - 65535` (slightly over 18 hours); default: `90`

`sesstimeout`

Enhanced MS-DOS and MS OS/2 clients— the interval, in seconds, that this client will wait before disconnecting a session from a server that is no longer responding.

Values: `10 - 65535` (slightly over 18 hours); default: `45`

`sizbigbuf`

Enhanced MS-DOS clients only — the size, in bytes, of big buffers used to receive large files or amounts of data.

(The `numbigbuf` keyword sets the number of buffers.)

Values: `0 – 65535`; default: `4096`

`sizcharbuf`

Enhanced MS-DOS and MS OS/2 clients only — The size, in bytes, of named pipe and character device buffers. Increase this number for better communication device performance. Each buffer takes up memory, so do not allocate more than you need. UNIX system servers do not support communication device queues.

Values: `64 – 4096`; default: `128` on an MS-DOS client, `512` on an MS OS/2 client

`sizerror`

MS OS/2 clients only — the size, in bytes, of this client's internal error buffer. Reduce this number from the default if you need more available memory and do not have frequent network errors.

Values: `256 – 4096`; default: `1024`

`sizworkbuf`

Enhanced MS-DOS and MS OS/2 clients only — The size, in bytes, of client buffers. Increase this number from the default if you need to transfer large chunks of data, such as database records, across the network. The value of this keyword setting should be the same for every client on the network.

On an Enhanced MS-DOS client used for administering the server, the value of this keyword affects the number of users and groups that you can specify when setting permissions for a resource. For example, the default value of 1024 allows you to specify 42 separate users and groups. If this limit becomes a problem, increase the value of this keyword.

Values: `64 - 4096` for an MS-DOS client, `1024 - 16384` (in multiples of 512) for an MS OS/2 client; default: `1024` for an MS-DOS client, `4096` for an MS OS/2 client

`umb`

MS-DOS clients only — loads the Workstation service (*netwksta.exe*) into upper memory blocks, as available.

Values: yes and no; default: yes

`wrkheuristics`

Enhanced MS-DOS and MS OS/2 clients only — Sets a wide variety of client fine-tuning options.

Values: a field of numeric characters, each with an independent meaning. On an MS-DOS client, the characters are numbered from 0 to 32, with characters 17 to 32 reserved for future use. On an MS OS/2 client, the characters are numbered from 0 to 54, with characters 35 to 54 reserved for future use.

Table C-1 describes characters 0 to 16 on an MS-DOS client, and Table C-2 describes characters 0 to 33 on an MS OS/2 client. Except where noted, each character is a binary digit, with 0 meaning "off" or "inactive," and 1 meaning "on" or "active."

The following four lines illustrate the defaults: Lines 1 and 2 show the character positions; Line 3 is the default on an MS-DOS client; Line 4 is the default on an MS OS/2 client.

```
1)                    1                   2                   3
2) 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
3) 1 1 1 1 2 1 1 0 1 2 0 0 2 0 1 0 2
4) 1 1 1 1 1 1 1 1 2 1 3 1 1 1 1 1 1 1 1 0 0 1 0 1 1 1 2 0 0 1 1 2 2 1
```

Table C-1: wrkheuristics Keyword Character Values — MS-DOS Client

Character	Description and Values
0	Turn on write-through bit on all open files. Default: 1
1	Do asynchronous write buffer and close operations. Default: 1
2	Specify whether NetBIOS performs a Send operation during power-on self-test. Default: 1 to allow NetBIOS to SEND
3	Use buffer size transfer as follows: 0 = limit transfer to local buffer size 1 = use two read operations for core read 2 = Use `Message Incomplete` error for transfer (may degrade system performance) Default: 1 This heuristic is used for communication with **core servers** (servers that use the core Server Message Block [SMB] protocols, such as pre-2.0 LAN Manager servers).

Table C-1: *Continued*

Character	Description and Values
4	Use buffer mode as follows (assuming that share access is permitted): 0 = always read the value of `bufsize` if request is smaller than `bufsize` 1 = use full buffer if file is open for read/write 2 = use full buffer if reading/writing sequentially Default: 2
5	Send a pop-up message to the screen on hard errors. Default: 1 to send pop-up messages
6	Big buffer read-ahead. If not enabled, performance may be degraded. Default: 1 to use big buffer read-ahead
7	Send process exit SMBs as follows: 0 = never 1 = always 2 = send based on RPDB structure Default: 0
8	Request opportunistic locking of files. This opens files on the server with "deny none" permissions, allowing faster buffering. If another client requests access to the same file, the server lets the first client flush data before providing the second access. Default: 1
9	Use Open And Read as follows:

Table C-1: *Continued*

Character	Description and Values
	0 = never 1 = Open and Read on files with RW access permissions 2 = Open and Read on files with RWX access permissions Default: 2
10	Controls MS-DOS commit calls as follows: 0 = flush buffers to server and wait for server to flush buffers to disk 1 = flush buffers to server and do not wait 2 = flush buffer when full or job is done Default: 1
11	Controls beeping while the client waits for a network request to be processed. The default is 0, which indicates that beeping is turned off. This value cannot be changed. Default: 0
12	Perform asynchronous read-ahead as follows: 0 = never 1 = at buffer end 2 = on second pass through a buffer Default: 2

Table C-1: *Continued*

Character	Description and Values
13	Controls three-way write, unlock, lock, and read SMB as follows: 0 = do not issue 1 = issue Default: 0
14	Controls use of raw data transfer SMB protocols as follows: 0 = do not use 1 = use Default: 1, change to 0 to use Remote Access
15	Controls the use of hook interrupt 21 (INT21) as follows: 0 hook INT21 1 don't hook INT21 Default: 0
16	Controls buffering with compatability mode opens. (For a Basic MS-DOS client, this corresponds to the **net start workstation /cb** option.) 0 no buffer 1 buffer only if no outstanding locks on the file 2 always buffer Default: 2

Table C-2: wrkheuristics Keyword Character Values — MS OS/2 Client

Character	Description and Values
0	Request opportunistic locking of files. This opens files on the server with "deny none" permissions, allowing faster buffering. If another client requests access to the same file, the server lets the first client flush data before providing the second access. Default: 1
1	Optimize performance for batch files. If this character is set to 1, character 0, opportunistic locking, must also be set to 1. Default: 1
2	Unlock and WriteUnlock asynchronously, as follows: 0 = never 1 = always 2 = only on a virtual circuit Default: 1 When a user unlocks a file, if Unlocks and WriteUnlocks are asynchronous, the user need not wait for the server to acknowledge, but can overlap local processing with the server's processing of the unlock (and transport time). Asynchronous Unlock and WriteUnlock is not used if write-through is set.
3	Close and WriteClose asynchronously, as follows: 0 = never 1 = always

Table C-2: *Continued*

Character	Description and Values
	2 = only on a virtual circuit Default: 1 When transferring large files, the client can get ahead of the server if all data transferred to the server is in its buffers but not processed to disk. When the server gets a Close or WriteClose request, it flushes all data to disk (or to the remaining system cache) before it processes and returns the Close response. When this character is set to 1, the client sends the Close but does not wait for the response, and a user can overlap local processing with server processing (write to disk at the same time). A popup message informs the user if all data is not written to disk.
4	Buffer named pipes and communication devices. Default: 1 Buffering the named pipe and communication devices protects information by putting it in a buffer. The workstation then reads the information from the buffer.
5	LockRead and WriteUnlock as follows: 0 = never 1 = always 2 = only on a virtual circuit Default: 1 Some database applications use a dummy file to control the real database file; the application locks the dummy file and reads only the real file. On a high-speed network this

Table C-2: *Continued*

Character	Description and Values
	should not matter, but on a slow network it could degrade performance. If you have a slow network and regularly use a database that uses a dummy file, consider setting this character to 0.
6	Use Open And Read. This heuristic combines Open and Read to get the first portion of a file at the same time the file is opened. On a slow network, set this character to 0 if you use many applications that read files randomly, rather than sequentially. Default: 1
7	Read ahead to sector boundary. A file system that is not sensitive to the location of information or the reading of partial disk sectors (or that has an active cache) performs better by reading ahead to a sector boundary. Default: 1
8	Use the chain send NetBIOS NCB as follows: 0 = never 1 = only if the server's buffer is larger than the client's 2 = always, to avoid copy Default: 2 A chained send enables sending data directly from the client's buffer to the transport driver, bypassing data copy. The transport driver design determines which setting is

Table C-2: *Continued*

Character	Description and Values
	optimum.
9	Buffer small read/write requests (reading and writing a full buffer) as follows: 0 = never 1 = always 2 = only on a virtual circuit Default: 1
10	Use buffer mode as follows (assuming that share access is permitted): 0 = always read the value of `bufsize` if request is smaller than `bufsize` 1 = use full buffer if file is open for read/write 2 = use full buffer if reading/writing sequentially 3 = buffer all requests that are smaller than `bufsize` Default: 3
11	Use RAW data transfer read/write SMB protocols. Default: 1
12	Use large RAW data transfer read-ahead buffer. Default: 1
13	Use large RAW data transfer write-behind buffer. Default: 1
14	Use read multiplex SMB protocols. Default: 1

Table C-2: *Continued*

Character	Description and Values
15	Use write multiplex SMB protocols. Default: 1
16	Use big buffer for large core reads. Default: 1
17	Set the read-ahead size as follows: 0 = read to sector boundary 1 = use a multiple of the size that the user is reading For example, if the user is reading 50-byte chunks of a 4096-byte buffer, LAN Manager reads ahead to fill the buffer to 4050 bytes. Default: 1
18	Set the write-behind size as follows: 0 = write to sector boundary 1 = use a multiple of the size that the user is writing Default: 1
19	Force 512-byte maximum transfers to and from core server. Default: 0

Table C-2: *Continued*

Character	Description and Values
20	Flush pipes and devices on DosBufReset or DosClose as follows: 0 = only files/devices opened by caller; spin until flushed 1 = only files/devices opened by caller; flush only once 2 = all files and short-term pipe/device I/O; spin until flushed 3 = all files and short-term pipe/device I/O; flush only once 4 = all files and pipe/device I/O; spin until flushed 5 = all files and pipe/device I/O; flush only once Default: 0
21	Use password encryption if the server supports it. Default: 1
22	Control log entries for multiple occurrences of an error. A recurring error can fill up the client's error log; you can use this heuristic to keep down the number of log entries by activating an interim table. If the value is 0, LAN Manager logs all error occurrences. A value from 1 to 9 sets the number of errors that can be held in the interim table, in which LAN Manager logs the 1st, 4th, 8th, 16th, and 32nd occurrences and every further 32nd occurrence of of the error. If the table is full, LAN Manager discards the error with the lowest number of occurrences to make room for the new error.

Table C-2: *Continued*

Character	Description and Values
	`Out of Resource` errors are logged only once per resource type regardless of the value of this heuristic. Default: 0
23	Buffer all files opened with "deny write" rights. Default: 1
24	Buffer all files opened with the R (read only) attribute. Default: 1
25	Read ahead when opening a file for execution. Sometimes reading an executable file can appear sequential when it is not. Default: 1
26	Handle Ctrl - C as follows: `0` = no interrupts allowed `1` = allow interrupts only on long-term operations `2` = always allow interrupts Default: 2
27	Force correct open mode when creating files on a core server. A core server opens a new file in compatibility mode, which is not ordinarily a problem. This heuristic forces the server to close the file and re-open it in the proper mode for a protected-mode client. Default: 0
28	Use the NetBIOS NoAck mode (transferring data without an immediate acknowledgement) as follows:

Table C-2: *Continued*

Character	**Description and Values**
	0 = never 1 = NoAck on send only 2 = NoAck on receive only 3 = NoAck on send and receive Default: 0
29	Send data along with SMB write block RAW data transfer requests. Default: 1
30	Send a popup message to the screen when the client logs an error, as follows: 0 = never 1 = on write fault errors only — no timeout 2 = on write fault and internal errors only — no timeout 3 = on all errors — no timeout 4 = (reserved) 5 = on write fault errors only — timeout 6 = on write fault and internal errors only — timeout 7 = on all errors — timeout Default: 1

Table C-2: *Continued*

Character	Description and Values
31	This heuristic is now reserved. Previously it controlled print buffer timeouts. See the `printbufftime` keyword in the [*workstation*] section.
32	Controls MS-DOS commit calls as follows: 0 = flush buffers to server and wait for server to flush buffers to disk 1 = flush buffers to server and do not wait 2 = flush buffer when full or job is done Default: 2
33	Controls the timeout value for performing logon validation from a domain controller as follows: 0 = 5 sec 1 = 15 sec 2 = 30 sec 3 = 45 sec 4 = 1 min 5 = 1 min, 30 sec 6 = 2 min 7 = 4 min 8 = 8 min 9 = 15 min Default: 1

Table C-2: *Continued*

Character	Description and Values
34	Allows compatibility with core level PCLP servers. Some PCLP servers send the date in word reversed order on the SMB getatr response. The heuristic controls how the client will handle SMBgetatr dates from core level servers on the network as follows: 0 Verify date with preference towards PCLP server 1 Verify date with preference towards SMB specification 2 Assume date is supplied as specified in SMB specification Default: 1

`validate` Allows you to long on without being validated by a logon server.

Values: yes (validation required) or no (no validation required); default: yes

`wrknets` Lists the names of the networks in which the workstation participates.

On Enhanced MS-DOS clients, networks are represented by LANA numbers. For information on LANA numbers, see the *LAN Manager Installation and Configuration Guide.*

On MS OS/2 clients, the names are also listed in the [*networks*] section.

You must separate multiple name entries with commas.

Values: `0 – 254` for an MS-DOS client, **net1** to the list of networks from the [*networks*] section for an MS OS/2 client; default: `0` networks for an MS-DOS client, `net1` for an MS OS/2 client

`wrkservices`

Specifies LAN Manager services to be started when the Client Program is started, for example, the Messenger service, which receives messages. The names of all the services that can potentially be started with this keyword are listed in the [*services*] section. Service names cannot be abbreviated.

Values: a list of services, separated by commas; default: `messenger,netpopup`

[messenger] Section

This section is on Enhanced MS-DOS and MS OS/2 clients only.

`logfile`

The location of the messages log file, relative to the *\lanman.dos\logs* directory on an Enhanced MS-DOS client or the *\lanman\logs* directory on an MS OS/2 client.

Default: `messages.log`

`nummsgnames`

Enhanced MS-DOS clients only — sets the maximum number of aliases for this client for receiving messages.

Values: `1` – `10`; default: `2`

`sizmessbuf`

The size, in bytes, of the buffers for sending and receiving messages. The client cannot receive messages larger than the value of this keyword. Increase this number from the default value if the client will be sending or receiving long messages. Increase this value to at least 512 on an Enhanced MS-DOS client if the client receives administrative alerts from a server. Larger buffers take more memory, so do not allocate larger buffers than you need.

Values: `128 – 62000` on an Enhanced MS-DOS client, `512 – 62000` on an MS OS/2 client; default: `256` on an Enhanced MS-DOS client, `4096` on an MS OS/2 client

[netshell] Section

This section applies to Enhanced MS-DOS and MS OS/2 clients only.

`autorestore`

Determines whether net connections saved from the last session will be restored at logon. Works with the `saveconnections` keyword to turn the persistent net connections feature on or off. This keyword is optional.

Values: yes and no; default: yes

`refresh`

MS OS/2 clients only — the interval, in seconds, at which the information in dialog boxes is updated. This keyword applies only to the Net Admin Interface.

Values: `0 - 65535` (slightly over 18 hours); default: `15`

`remote`

MS OS/2 clients only — the servername of the default server to administer using the **net admin** command.

Default: none

`saveconnections`

Determines whether net connections will be saved for restoration at a later logon. Works with the `autorestore` keyword to turn the persistent net connections feature on or off. This keyword is optional.

Values: yes and no; default: yes

`savewinlogonname`

Enhanced MS-DOS clients only — allows you to save the username you log in with in Windows to be used as the default the next time you log in.

Values: yes (save this name) and no (don't save this name); default: no

`username`

The default username used when logging on to the network unless the user specifies another. A username can be up to 20 characters long and can include letters, numbers, and the following characters:
! # $ % & ( ) - . @ ^ _ ` { } ~
Message aliases can have only 15 characters, so a longer username does not receive messages.

Default: none

[loadopts] Section

This section applies to Enhanced MS-DOS clients only. This section allows you to select how LAN Manager services are loaded into memory. By default, the services you specify in the [*services*] section are loaded into upper memory blocks (umbs) as they are available.

In the [*loadopts*] section, you can set each service to load either **low** or **umb**.

The format is as follows:

```
    service = {low | umb}
```

[node] Section

This section applies to MS OS/2 clients only.

This section specifies the default configuration values for the Node service of the Microsoft TCP/IP extensions for the LAN Manager Domain Services for TCP/IP. Since the Node service requries at least one LAN Manager 2.2 server running the MS OS/2 operating system, refer to the MS OS/2 server documentation for additional information.

[services] Section

This section applies to Enhanced MS-DOS and MS OS/2 clients only.

If a path used in this section does not start with a drive name or a backslash (\), it is assumed to be relative to the *lanman* directory.

`chknet`

Enhanced MS-DOS clients only — the location of the program that checks to see that the network has been installed.

Default: `netprog\chknet.exe`

`encrypt`

Enhanced MS-DOS clients only — the location of the password encryption service.

Default: `services\encrypt.exe`

`messenger`

The location of the Messenger service initialization program.

Default: `services\msrv.exe` on an MS-DOS client, `services\msrvinit.exe` on an MS OS/2 client

`minses`

Enhanced MS-DOS clients only — the location of the **minses** program, which installs the INT 2A interface used by NetBIOS applications.

Default: `services\minses.exe`

`netbind`

The location of the Netbind Program, which causes the Protocol Manager to bind together the protocol and network adapter drivers.

Default: `drivers\protman\netbind.exe`

`netpopup`

The location of the NetPopup Program.

Default: `services\netpopup.exe`

`prtsc`

Enhanced MS-DOS clients only — The location of the prtsc utility, which is used to flush the print spooler when an application fails to send an end-of-job signal to the printer. There is no [*prtsc*] section in *lanman.ini*.

Default: `netprog\prtsc.exe`

`workstation`

The location of the client initialization program.

Default on an Enhanced MS-DOS client: `netprog\netwksta.exe`

Default on an MS OS/2 client: `services\wksta.exe`

[version] Section

`lan_manager` The numeric value of this client's software release.

Default: `2.2`

Chapter D

Appendix D: Understanding the NVAlert Service

Overview

With the NVAlert service installed on a server on a LAN Manager network, the server can automatically report error and status information to an IBM NetView network-management host. As a network administrator, you only have to start and stop the service.

Alerts

The NVAlert service uses alerts to report information to an IBM NetView network-management host. Programmers writing host applications that interact with the alerts the NVAlert service generates must know the syntax, structure, and meaning of those alerts.

This section lists NVAlert service alerts with code points that were approved by IBM as of April, 1991. If your NetView software does not include these code points, contact IBM or add the code points to your host file.

LAN Manager Alerts and Errors

Many of the alerts listed in this section are derived from LAN Manager alerts and errors. The following tables show the relationship between LAN Manager events and NVAlert service alerts.

LAN Manager Alerts

Table D-1 lists LAN Manager Admin alerts that the NVAlert service monitors and maps into NetView alerts.

Table D-1: LAN Manager Admin Alerts

LAN Manager admin Alert	Alert number	Alert class
ALERT_Disk_Full	3000	Disk is nearly full
ALERT_ErrorLog	3001	Error log frequency is too high
ALERT_NetIO	3002	Net IO error frequency is too high
ALERT_Logon	3003	Password violation
ALERT_Access	3004	Access violation
ALERT_ErrorLogFull	3006	Error log is full
ALERT_ErrorLogFull_W	3007	Error log is nearly full
ALERT_AuditLogFull	3008	Audit log is full
ALERT_AuditLogFull_W	3009	Audit log is nearly full
ALERT_CloseBehindError	3010	Disk error occurred
ALERT_AccessShareSec	3012	Access violation
ALERT_PowerOut	3020	Power is out
ALERT_PowerBack	3021	Power is back
ALERT_PowerShutdown	3022	Power is shut down

Table D-1: *Continued*

LAN Manager admin Alert	Alert number	Alert class
ALERT_HardErr_Server	3026	Disk error occurred
ALERT_LocalSecFail1	3027	Local security exposure is corrupt
ALERT_LocalSecFail2	3028	Local security exposure is missing
ALERT_LocalSecFail3	3029	Local security failure
ALERT_AcctLimitExceeded	3033	User account limit reached
ALERT_NetLogonFailedPrimary	3034	Net logon failed on the primary
ALERT_NetLogonAuthDCFail	3035	Net logon authentication on domain controller failed

LAN Manager Errors

Table D-2 lists LAN Manager errors that the NVAlert service monitors and maps into NetView alerts.

Table D-2: LAN Manager Errors

LAN Manager error log alerts	Error number	Alert class
NELOG_Resource_Shortage	3101	Parameter is set too low
NELOG_Ncb_TooManyErr	3126	Parameter is set too low
NELOG_Lazy_Write_Err	3180	Disk error occurred
NELOG_LocalSecGeneralFail	3186	Local security failure
NELOG_NetWkSta_No_Resource	3191	Parameter is set too low
NELOG_NetWkSta_Write_Behind_Err	3196	Disk error occurred
NELOG_Srv_Thread_Failure	3204	Parameter is set too low
NELOG_Srv_Close_Failure	3205	Disk error occurred
NELOG_DiskFT	3221	Disk error occurred
NELOG_FT_ErrLog_Too_Large	3258	Error log is full

Printer Alerts

The NVAlert service also monitors printer alerts. The service checks bits in the printer status. If any of the bits listed in the following table are set, the service generates the corresponding alert.

Table D-3: Printer Alerts

Printer status bit manifest	Value	Alert class
PRJ_INTERV	0x0008	Printer needs attention
PRJ_ERROR	0x0010	Print error occurred
PRJ_DESTOFFLINE	0x0020	Printer needs attention
PRJ_DESTPAUSED	0x0040	Printer needs attention
PRJ_NOTIFY	0x0080	Print error occurred
PRJ_DESTNOPAPER	0x0100	Printer has no paper
PRJ_DESTFORMCHG	0x0200	Printer needs attention
PRJ_DESTCRTCHG	0x0400	Printer needs attention
PRJ_DESTPENCHG	0x0800	Printer needs attention

NVAlert Service Alerts

This section describes each alert the NVAlert service sends to a NetView host. Each alert description includes all or most of the following subfields.

Table D-4: NVAlert Service Descriptions

Subfield	Description
Alert ID	A unique number that identifies the alert.
Alert Type	The state of the alert— impending (warning), permanent (requires intervention), temporary (already corrected by software), or unknown problem.
Alert Description	A full description of the alert.
Probable Causes	List of factors that might have caused the alert.
User Causes	The user operation, if any, that might have caused the alert.
Recommended Actions (User)	Corrective measures for an alert caused by a user.
Install Causes	The install operation, if any, that may have caused the alert.
Recommended Actions (Install)	Corrective measures for an alert generated during installation.
Failure Causes	Any other operations that may have caused the alert.

Table D-4: *Continued*

Subfield	Description
Detailed Data	Can appear under User Causes, Install Causes, or Failure Causes. Gives detailed information about the possible cause in each instance.

Note: The NetView default alert display filter blocks temporary and impending alerts from view. To ensure that the NetView host recognizes the temporary and impending alerts that the NVAlert service sends to it, you must disable the default alert display filter.

The description for some of the code points in the following alerts contain the item "(sf82)." This item indicates a subfield (subfield number 82) that is given by the detailed data subfield when the alert occurs. In some instances, the detailed data subfield contains the item "(no display)." This item means that the detailed data string is empty.

Table D-5: Access Violation Alert

Subfield	Value or code point	Description
Alert ID	0x4CD65E2F	–
Alert Type	0x01	Permanent
Alert Description	0xC007	Unauthorized access attempted
Probable Causes	0x7030	File server user
User Causes	0x7199	Unauthorized access attempted
	0xF8A0	Problem detected by (sf82)
Detailed Data (User)	0x95	File server name
Recommended Actions (User)	0x3002 0x0164	Contact security control Review the server's audit trail
Install Causes	0x1717:	Attempted resource access violations threshold set too low
Recommended Actions (Install)	0x310A 0x150F	Contact server administrator Check threshold limit and change if set too low
Failure Causes	–	None

Table D-6: Audit Log Is Full Alert

Subfield	Value or code point	Description
Alert ID	0xBD285A1B	–
Alert Type	0x01	Permanent
Alert description	0x5108	Audit log limit reached
Probable Causes	0x0012 0x7030	File server File server user
User Causes	0x73A0	File full (sf82)
Detailed Data (User)	0xD0 0xF8A0	Filename Problem detected by (sf82)
	0x95	File server name
Recommended Actions (User)	0x310A	Contact server administrator
	0x101B	Print and then clear audit log
	0x0164	Review server's audit trail
Install causes	0x1719	Audit log size set too low
Recommended Actions (User)	0x310A	Contact server administrator
	0x0165	Check audit log size and change if set too low
	0x101D	Reduce types of audit entries logged
Failure Causes	–	None

Table D-7: Audit Log Is Nearly Full Alert

Subfield	Value or code point	Description
Alert ID	0x5285D2C2	–
Alert Type	0x11	Impending
Alert Description	0x510A	Audit log file almost full
Probable Causes	0x0012 0x7030	File server File server user
User Causes	0x73A3	File almost full (sf82)
Detailed Data (User)	0xD0 0xF8A0 0x95	Filename Problem detected by (sf82) File server name
Recommended Actions (User)	0x310A	Contact server administrator
	0x101B	Print and then clear audit log
	0x0164	Review server's audit trail
Install Causes	0x1719	Audit log size set too low
Recommended Actions (User)	0x310A	Contact server administrator
	0x0165	Check audit log size and change if set too low
	0x101D	Reduce types of audit entries logged
Failure Causes	–	None

Table D-8: Disk Error Occurred Alert

Subfield	Value or code point	Description
Alert ID	0x55833F16	–
Alert Type	0x01	Permanent
Alert Description	0x2201	Possible file corruption
Probable Causes	0x0501	Storage subsystem
User Causes	–	None
Install Causes	–	None
Failure Causes	0x0501 0xF1A1	Storage subsystem Disk write errors on (sf82)
Detailed Data	0xD0 0x8C 0xF8A0 0x95	Filename* Volume or filename* Problem detected by (sf82) File server name
Recommended Actions	0x310A	Contact server administrator
	0x0135 0x1005	Verify file is valid Perform disk file error recovery

*The filename is included for the following Admin alert condition:

```
ALERT_CloseBehindError
```

The filename is included for the following error log entries that are sent as Errlog alerts:

```
NELOG_NetWksta_Write_Behind_Err
NELOG_SRV_Close_Failure
```

The volume name is included for the following Admin alert condition:

```
ALERT_HardErr_Server
```

The volume name is included for the following error log entry that is sent as an Errlog alert:

```
NELOG_Lazy_Write_Err
```

Table D-9: Disk Is Nearly Full Alert

Subfield	Value or code point	Description
Alert ID	0x0206D99A	–
Alert Type	0x11	Impending
Alert Description	0x5002	Resource nearing capacity
Probable Causes	0x0501 0x7030	Storage subsystem File server user
User Causes	0x0102	Insufficient storage-media space
	0xF0A0	Insufficient storage-media space available for (sf82)
Detailed Data (User)	0x29 0xF8A0 0x95	Disk drive Problem detected by (sf82) File server name
Recommended Actions (User)	0x1019 0x1020	Purge unused files Increase storage-media capacity

Table D-9: *Continued*

Subfield	Value or code point	Description
	0x310A	Contact server administrator
Install Causes	0x1715 0x1715	Minimum free disk space Threshold set too high
Recommended Actions (Install)	0x310A 0x1511	Contact server administrator Check threshold limit and change
Failure Causes	–	None

Table D-10: Error Log Frequency Is Too High Alert

Subfield	Value or code point	Description
Alert ID	0x6851CDD8	–
Alert Type	0x12	Severity unknown
Alert Description	0x510C	File server error limit reached
Probable Causes	0x0012	File server
User Causes	–	None
Install Causes:	0x171B	Predefined resource threshold set too low
	0x171C	File server error threshold set too low
	0xF8A0	Problem detected by (sf82)
Detailed Data	0x95	File server name
Recommended Actions	0x310A 0x0167 0x150F	Contact server administrator Review server error log Check threshold limit and change if set too low
Failure Causes	0x3700	LAN Manager component
Recommended Actions	0x310A 0x0167	Contact server administrator Review server error log

Table D-11: Error Log Is Full Alert

Subfield	Value or code point	Description
Alert ID	0x74B32343	–
Alert Type	0x01	Permanent
Alert Description	0x5107	Error log limit reached
Probable Causes	0x0012	File server
	0x7030	File Server User
User Causes	0x73A0	File full (sf82)
Detailed Data (User)	0xD0	Filename
	0xF8A0	Problem detected by (sf82)
	0x95	File server name
Recommended Actions (User)	0x101A	Print and then clear error log
	0x0167	Review server error log
	0x310A	Contact server administrator
Install Causes	0x1718	Error log size set too low
Recommended Actions (Install)	0x310A	Contact server administrator
	0x0165	Check error log size and change if set too low
Failure Causes	–	None

Table D-12: Error Log Is Nearly Full

Subfield	Value or code point	Description
Alert ID	0x6FA9357A	–
Alert Type	0x11	Impending
Alert Description	0x5109	Error log file almost full
Probable Causes	0x0012 0x7030	File server File server user
User Causes	0x73A3	File almost full (sf82)
Detailed Data (User)	0xD0 0xF8A0 0x95	Filename Problem detected by (sf82) File server name
Recommended Actions (User)	0x101A 0x0167 0x310A	Print and then clear error log Review server error log Contact server administrator
Install Causes	0x1718	Error log size set too low
Recommended Actions (Install)	0x310A 0x0165	Contact server administrator Check error log size and change if set too low
Failure Causes	–	None

Table D-13: Local Security Exposure Is Corrupt

Subfield	Value or code point	Description
Alert ID	0xE5EF11A9	–
Alert Type	0x01	Permanent
Alert Description	0xC000	Security event
Probable Causes File server account system file	0x8020	
	0x0501	Storage subsystem
User Causes	–	None
Install Causes	–	None
Failure Causes	0x0501 0x10A3	Storage subsystem (sf82) is corrupt
Detailed Data (Failure)	0x76 0xF8A0 0x95	Security database file Problem detected by (sf82) File server name
Recommended Actions (Failure)	0x3002:	Contact security control representative
	0xF0A1	(sf82) was restored from backup file
	0x10A5	Review (sf82) and update as required

Table D-14: Local Security Exposure Is Missing

Subfield	Value or code point	Description
Alert ID	0xE5E811A9	–
Alert Type	0x01	Permanent
Alert Description	0xC000	Security event
Probable Causes	0x8020	File server account system file
	0x0501	Storage subsystem
User Causes	–	None
Install Causes	–	None
Failure Causes	0x0501	Storage subsystem
	0x10A4	(sf82) not found
Detailed Data (Failure)	0x76	Security database file
	0xF8A0	Problem detected by (sf82)
	0x95	File server name
Recommended Actions (Failure)	0x3002:	Contact security control representative
	0xF0A1:	(sf82) was restored from backup file
	0x10A5:	Review (sf82) and update as required

Table D-15: Local Security Failure

Subfield	Value or code point	Description
Alert ID	0x8F579A61	–
Alert Type	0x01	Permanent
Alert Description	0xC000	Security event
Probable Causes	0x8020 0x0501	File server account system file Storage subsystem
User Causes	–	None
Install Causes	–	None
Failure Causes	0x0501 0x10A3 (sf82) is corrupt	Storage subsystem
Detailed Data (Failure)	0x76 0x10A4 (sf82) not found 0x76 0xF8A0 0x95	Security database file Security database file Problem detected by (sf82) File server name
Recommended Actions (Failure)	0x3002	Contact security control representative
	0xF0A2 0x10A6	No backup available for (sf82) Create new (sf82)

Table D-16: Net I/O Error Frequency Is Too High

Subfield	Value or code point	Description
Alert ID	0xC7B05EB3	–
Alert Type	0x12	Unknown
Alert Description	0x510D	Network I/O error limit reached
Probable Causes	0x3700	LAN Manager component
	0x0012	File server
User Causes	–	None
Install Causes	0x171D	Network I/O threshold set too low
	0xF8A0	Problem detected by (sf82)
Detailed Data (Install)	0x95	File server name
Recommended Actions (Install)	0x310A	Contact server administrator
	0x150F	Check threshold limit and change if set too low
Failure Causes	0x3700	LAN Manager component
	0x3760	File server
	0xF8C0	Failing component is identified by (sf82)
Detailed Data (Failure)	0x73	Configuration parameter
	0x00	(no display)
Recommended Actions (Failure)	0x310A	Contact server administrator
	0x310B	Contact network administrator
	0x0167	Review server's error log
	0x00B0	Perform problem determination procedures for (sf82)
	0x1004	Perform LAN Manager problem-recovery procedures

Table D-17: Net Logon Authentication on Domain Controller Failed

Subfield	Value or code point	Description
Alert ID	0x068ECAF7	–
Alert Type	0x01	Permanent
Alert Description	0xC008	Access to domain controller denied
Probable Causes	0x8020 0x8021	File server account system file Domain controller account system file
User Causes	0x711B 0x711C	File server password changed Difference between system clock times unacceptable
	0xF8A0	Problem detected by (sf82)
Detailed Data (User)	0x95	File server name
Recommended Actions (User)	0x3103	Contact LAN Manager administrator
	0x103D	Synchronize password at file server and domain controller
	0x103F	Synchronize system clock times
Install Causes	–	None
Failure Causes	0x12AD	(sf82) restored and not synchronized
Detailed Data (Failure)	0x78	Account system file
Recommended Actions (Failure)	0x3103 0x141E 0x10A7	Contact LAN Manager administrator Stop and restart server logon service Restore (sf82) on domain controller and file server from backup file

Table D-18: Net Logon Failed on the Primary

Subfield	Value or code point	Description
Alert ID	0x380C4690	–
Alert Type	0x12	Unknown
Alert Description	0x3270	Unable to contact domain controller
Probable Causes	0x3708	Domain controller
User Causes	0x601A	Domain controller stopped or powered off
	0xF8A0	Problem detected by (sf82)
Detailed Data (User)	0x95	File server name
Recommended Actions (User)	0x3103	Contact LAN Manager administrator
	0x0168	Check domain controller
	0x141D	Power on or restart
Install Causes	–	None
Failure Causes	0x3708	Domain controller
	0x3700	LAN Manager component
	0x3760	File server
Recommended Actions (Failure)	0x3103	Contact LAN Manager administrator
	0x0167	Review server's error log

Table D-19: Parameter Is Set Too Low

Subfield	Value or code point	Description
Alert ID	0x88AC3327	--
Alert Type	0x01	Permanent
Alert Description	0x5003	Configurable capacity limit reached
Probable Causes	0x1057 0x8005	Resource limit reached Server configuration
User Causes	0x7144 0xF8A0	Resource not available Problem detected by (sf82)
Detailed Data (User)	0x95	File server name
Recommended Actions (User)	0x1206	Wait and then retry
Install Causes	0x17C0	Threshold value set too low (sf82)
Detailed Data (Install)	0x73 0x75 0x3700	Configuration parameter Parameter value LAN Manager configuration error
Recommended Actions (Install)	0x310A 0x150F	Contact server administrator Check threshold limit and change if set too low
	0x1503	
Correct configuration		
Failure Causes	--	None

Table D-20: Password Violation

Subfield	Value or code point	Description
Alert ID	0xB57BD9C1	--
Alert Type	0x01	Permanent
Alert Description	0xC006	Invalid password
Probable Causes	0x7030	File server user
User Causes	0x7199 0xF8A0	Unauthorized access attempted Problem detected by (sf82)
Detailed Data (User)	0x95	File server name
Recommended Actions (User	0x3002 0x0164	Contact security control Review the server's audit trail
Install Causes	0x1716	Logon violation threshold set too low
Recommended Actions (Install)	0x310A 0x150F	Contact server administrator Check threshold limit and change if set too low
Failure Causes	--	None

Table D-21: Power Is Back

Subfield	Value or code point	Description
Alert ID	0x92C112E7	–
Alert Type	0x02	Temporary
Alert Description	0xA000	Problem resolved
Probable Causes	0x0220	Main AC power supply
User Causes	–	None
Install Causes	–	None
Failure Causes	0x0220 0xF8A0	Main AC power supply Problem detected by (sf82)
Detailed Data (Failure)	0x95	File server name
Recommended Actions (Failure)	0x0700	No action necessary

Table D-22: Power Is Out

Subfield	Value or code point	Description
Alert ID	0xF9D99F51	–
Alert Type	0x11	Impending
Alert Description	0x1412	Loss of all sources of electrical power
Probable Causes	0x0220 0x0012	Main AC power supply File server
User Causes	--	None
Install Causes	--	None
Failure Causes	0x0220 0xF101	Main AC power supply Server is running on battery power
	0xF8A0	Problem detected by (sf82)
Detailed Data (Failure)	0x95	File server name
Recommended Actions (Failure)	0x310A	Contact server administrator
	0x0200 0x1B11	Check power Prepare for server shutdown

Table D-23: Power Is Shut Down

Subfield	Value or code point	Description
Alert ID	0x447FB2D3	–
Alert Type	0x01	Permanent
Alert Description	0x1412	Loss of all sources of electrical power
Probable Causes	0x0220 0x0012	Main AC power supply File server
User Causes	–	None
Install Causes	–	None
Failure Causes	0x0220 0x0210 0xF07C 0xF1A7	Main AC power supply Battery Backup battery critically low (sf82) was shut down
Detailed Data (Failure)	0x95 0xF8A0 0x95	File server Problem detected by (sf82) File server name
Recommended Actions (Failure)	0x310B 0x0200	Contact network administrator Check power

Table D-24: Printer Has No Paper

Subfield	Value or code point	Description
Alert ID	0x67643422	--
Alert Type	0x01	Permanent
Alert Description	0x9202	Out of paper
Probable Causes	0x6210 0x7004	Printer User
User Causes	0x5303 0xF8A0	Out of paper Problem detected by (sf82)
Detailed Data (User)	0x95	File server name
Recommended Actions (User)	0x1606	Add paper
Install Causes	--	None
Failure Causes	0xF8C0	Failing component is identified by (sf82)
Detailed Data (Failure)	0x00 0x00	(no display)* (no display)*

*The failing component is identified by the servername and printer queue name.

Table D-25: Printer Needs Attention

Subfield	Value or code point	Description
Alert ID	0x855636EF	–
Alert Type	0x01	Permanent
Alert Description	0x9000	Operator intervention required
Probable Causes	0x6210 0x0011 0x1011 0x7010 0x7004	Printer Printer server Printer server program Printer operator User
User Causes	0x6013 0x6001 0xF8A0	Printer not ready Device offline Problem detected by (sf82)
Detailed Data (User)	0x95	File server name
Recommended Actions (User)	0x1301	Wait until printer is ready and then retry.
Install Causes	–	None
Failure Causes	0xF8C0	Failing component is identified by (sf82)
Detailed Data (Failure)	0x00 0x00	(no display)* (no display)*

*The failing component is identified by the servername and printer queue name.

Table D-26: Print Error Occurred

Subfield	Value or code point	Description
Alert ID	0x4DC7A231	–
Alert Type	0x01	Permanent
Alert Description	0x1201	Print error
Probable Causes	0x6210 0x0011	Printer Print server
User Causes	–	None
Install Causes	–	None
Failure Causes	0x6210 0xF8C0	Printer Failing component is identified by (sf82)
Detailed Data (Failure)	0x00 0x00 0xF8A0 0x95	(no display)* (no display)* Problem detected by (sf82) File server name
Recommended Actions (Failure)	0x310B	Contact network administrator

*The failing component is identified by the servername and printer queue name.

Table D-27: User Account Limit Reached

Subfield	Value or code point	Description
Alert ID	0x868BEA02	--
Alert Type	0x11	Impending
Alert Description	0x510B	Account limit reached
Probable Causes	0x7030	File server user
User Causes	0x71A4	(sf82) reached account limitation
Detailed Data (User)	0x98 0xF8A0 0x95	User name Problem detected by (sf82) File server name
Recommended Actions (User)	0x310A 0xF00C 0x1039	Contact server administrator Notify user Terminate user session
Install Causes	0x171A 0x17C1	User account limit set too low (sf82) is set at (sf82)
Detailed Data (Install)	0x73 0x75	Configuration parameter Parameter value
Recommended Actions (Install)	0x310A 0x0166	Contact server administrator Increase user account limitation

Glossary

absolute path

A pathname whose reference to a file or directory does not depend on the current drive or directory. In the DOS and OS/2 operating systems, an absolute path starts at the drive ID with a drive letter, colon, and backslash (for example, C:\ ). In the UNIX operating system, it starts at the *root* directory with a forward slash (/). *See also* network path; relative path.

access permissions

See permissions.

account

See user account.

accounts database

See user accounts database.

accounts operator

An operator privilege that allows a user (with user privilege) to create, remove, and modify user accounts (except those with admin privilege) and groups. *See also* operator privilege; print operator; server operator.

Activity Monitor

A display on the server console that shows server and client activity on the network.

ADMIN$* An administrative resource that enables remote administration on servers. A server's *ADMIN$ resource must be shared for the server to be administered remotely. *See also IPC$.*

admin alert A message from LAN Manager about server and resource use. *See also* error alert; printer alert.

administrative resource A resource used when network users and administrators perform certain tasks on the server, including viewing the resources the server is sharing, administering the server remotely, and running shared applications. Administrative resources include *ADMIN$*, *IPC$*, and the disk administrative resources. How these resources are shared determines how users can perform tasks.

administrator The individual responsible for managing the network. This person typically configures the network, maintains shared resources and security, assigns passwords and privileges, and helps users. *See also* operator privilege.

admin privilege The privilege level that allows a user at a server to use all administrative commands and all the resources shared by that server, regardless of the resource access permissions for the user. Users with admin privilege belong to the special group *admins*. *See also* permissions; privilege level.

alert A message that LAN Manager sends when certain specified events occur. The three classes of alerts are admin alerts, error alerts, and printer alerts. A computer must be running the Messenger service to receive alerts.

Alerter service A LAN Manager service that enables a server to send error messages and alerts to a designated list of users.

alias A name under which a user or computer can receive messages. Each client's computername is automatically added to its list of aliases. Other aliases can be added with the **net name** command. An alias is not the same as a username, although a username can be added as an alias.

auditing The process in which LAN Manager records an entry in the audit trail whenever a user accesses a resource in a certain way or logs on to the network.

audit trail A file containing a record of specified events on the network, such as when a user logs on or accesses a resource.

backup domain controller A server in a domain that keeps and uses a copy of the domain's user accounts database to validate logon requests. *See also* member server; Netlogon service; primary domain controller.

banner page *See* separator page.

batch program A file consisting of executable commands. *See also* filename extension.

broadcast message A message sent to all users in a domain or to all users on the LAN. *See also* Messenger service.

check box A field in a Net Admin Interface dialog box, used to enable or disable an option.

client A computer from which a user accesses shared network resources. Also known as workstation.

clone To use an existing user account or group as a template for a new user account or group.

Command Line Net Interface LAN Manager's command-oriented administrative interface. This interface consists of **net** commands that can be entered at a client's (Enhanced) DOS or OS/2 prompt or at the UNIX system prompt at the server console, at a client on the LAN running a terminal emulator, or at a remote terminal.

computername The name by which the LAN identifies a server or a client. Each computername must be unique on the network.

connection The logical link between a client and a shared resource on a server. A connection can be made by assigning a local devicename on the client to a resource shared on a server. A connection can also be made when the resource is accessed by using a network path with a command or from an application. *See also* session.

continue To restart a LAN Manager service that was paused.

country code A code in a user account that specifies the language in which the server sends messages to the user.

current focus The server or client that is the focus of activity when using the Net Admin Interface.

default permissions The permissions assigned to the parent directory or drive if no permissions are assigned explicitly for a directory or file. If no permissions are assigned for a printer queue or named pipe, the default permissions are the permissions assigned to the *PRINT* or *PIPE* resource.

device A piece of hardware connected to a computer, such as a disk drive or printer.

devicename The name by which a computer identifies a printer, disk, or other device. Disk devices are identified by a drive letter followed by a colon (for example, C:). For a client, a printer or other device is identified by the port to which it is connected, for example, LPT1:.

dialog box A data-entry form that appears on the Net Admin Interface when you select a command from a menu (except for `Exit`). Dialog boxes typically present a number of options from which to select or text boxes for entry of text. Completing some dialog boxes causes another dialog box to appear.

disk administrative resource The administrative resource, C$, that represents a server's disk drives. An administrator performing remote administration can use this resource to access all the files on the server's disk drives. Only an administrator can connect to the disk administrative resource. *See also ADMIN$; IPC$.*

disk resource A shared disk device. LAN Manager can share a directory tree or a single directory as a disk resource. *See also* devicename.

domain An administrative grouping of servers and clients. *See also* logon validation.

domain controller *See* backup domain controller; primary domain controller.

DOS (Disk Operating System) The operating system that supports some LAN Manager clients.

error alert A message that LAN Manager sends to the error log when a LAN or system error occurs. *See also* admin alert; printer alert.

error log A file that stores error messages.

escape code An instruction sent from a computer to a printer.

filename extension A period and up to three characters appended to a filename, often indicating what kind of file is named and sometimes required by the operating system or an application. For example, DOS batch programs always have the extension *.bat*.

group Under user-level security, a set of user accounts sharing common permissions for one or more resources. A group is used in the same way as a username when assigning permissions for resources. Individually assigned user permissions take precedence over those assigned to groups of which the user is a member.

guest account An account on a server running user-level security that allows a user without an individual user account to access the server's resources.

guest privilege A privilege level that allows a user to use network resources, view information about a server's shared resources and the status of printer queues, and send and receive messages. Users with guest privilege belong to the special group *guests*. *See also* permissions; privilege level.

hidden server A server that is part of a domain, but does not appear in the list of servers.

home directory A directory assigned to a user on a server running user-level security.

inherited permissions Permissions that can be assigned to an entire directory tree within a shared disk resource.

interprocess communication (IPC) Communication among the component processes of a program, between different computers running parts of a single program, or between two programs working together. *See also* named pipe.

***IPC$*** An administrative resource that controls how interprocess communication works on servers. A server's *IPC$* resource must be shared before the resources shared by the server can be viewed on the network, before the server can be administered remotely, and before users can use shared applications on the server. *See also ADMIN$*; named pipe.

keyword An item in the *lanman.ini* file, setting a LAN Manager option.

LAN (local area network) A group of computers, linked by cable or other physical media, that lets users share information and equipment.

lanman.ini The LAN Manager initialization file on each server and client. The values of the keywords in this file determine the option settings for computers on the network.

listener program
A UNIX daemon that monitors the network, receiving and accepting incoming connection requests, and then invoking the service that is requested.

lmx.ctrl
The master control process for LAN Manager. Under normal circumstances you should not modify this process.

lmx.srv
Processes that control individual client sessions and are managed by lmx.ctrl.

local
Used to describe the server or client at which the user or administrator is currently working, or a device or resource connected directly to that server or client. *See also* remote.

local area network
See LAN.

local user
The user or administrator working at the local computer's keyboard.

lock out accounts
Used to specify the maximum number of failed logon attemps users are allowed before their accounts are disabled (locked out).

log off
To end a user's session on the network.

log on
To start a user's session on the network by providing a username and password. When connecting to resources, LAN Manager validates the username and password before allowing access. In a domain running logon validation, the username and password must match a valid user account on the primary domain controller.

logical drive
Any resource given a drive designation (such as D:), for example, a client's disk partition or redirected drive, which makes a connection to a remote disk resource.

logon domain
The domain specified when logging on to the network.

logon hours
The days and times during which a user can access a server's resources.

logon restrictions
A user's specified logon hours and the list of clients from which the user can access a server's resources.

logon script
A batch program containing LAN Manager and operating system commands used to configure clients. Logon scripts can be written for one or more users. When the user logs on, the logon script runs at the user's client.

logon server The server that processes a user's logon request — the primary domain controller or a backup domain controller. *See also* Netlogon service.

logon validation A means of verifying the identities of users when they log on to the network and of centralizing the user accounts database for a domain, with copies distributed to servers throughout the domain. *See also* Netlogon service.

member server A server in a domain that keeps and uses a copy of the domain's user accounts database but does not validate logon requests. *See also* backup domain controller and primary domain controller.

menu bar The bar across the top of the Net Admin Interface that contains the names of menus.

message alias *See* alias.

message forwarding The use of aliases to reroute messages from one client or server to another.

message line A line at the bottom of the Net Admin Interface, providing information about the current menu, command, dialog box, or task.

message log A file that stores messages.

message popup A box that displays messages received from other network users when the Messenger and NetPopup services are running.

Messenger service A LAN Manager client service that enables a client to receive messages from other network users. This service can also store messages in a message log file.

MS-DOS (Disk Operating System) The operating system that supports some LAN Manager clients.

MS OS/2 (Operating System/2) The operating system that supports some LAN Manager clients.

named pipe A connection used to transfer data between separate processes on the same or different computers. Named pipes are the foundation of interprocess communication. An administrator can set permissions on named pipes, but only LAN Manager and network applications can create them. *See also IPC$*.

Net Admin Interface LAN Manager's menu-oriented administrative interface, available at a client running OS/2.

Net Admin Interface for Windows LAN Manager's menu-oriented administrative interface, available at a client running Enhanced DOS.

Netlogon service A LAN Manager service that implements logon validation. When a server in a domain runs the Netlogon service, the username and password supplied by each user who attempts to log on in the domain are checked. All servers participating in logon validation run the Netlogon service, which replicates the user accounts database to these servers. *See also* backup domain controller; member server; primary domain controller; standalone server.

NetPopup service A LAN Manager client service that displays messages on the client's computer screen when they arrive from other network users or from the server.

network path The computername of a server followed by the sharename of a shared resource and, optionally, a relative path. *See also* UNC, absolute path, and relative path.

NVAlert Service A LAN Manager service that allows a server on a LAN Manager network to report error and status information to an IBM NetView network management host.

operator privilege A privilege assigned to a user that allows the performance of certain administrative tasks. *See also* accounts operator; print operator; server operator.

option button One of a set of options in a Net Admin Interface dialog box. You can select only one option from the set.

OS/2 (Operating System/2) The operating system that supports some LAN Manager clients.

parallel printer A printer attached to a computer's parallel port. *See also* devicename.

pause To suspend a LAN Manager service. When a service is paused, current requests are not stopped, but new requests are not allowed. *See also* continue.

permissions Settings that define the kinds of action a user can take with a specific shared resource. Under user-level security, each user is assigned permissions for each resource. Under share-level security, each resource is assigned permissions, which apply to all users who can access the resource.

primary domain controller The server at which the master copy of a domain's user accounts database is maintained. The primary domain controller also validates logon requests. *See also* backup domain controller; member server.

printer alert A message that LAN Manager sends about a printer event to the user who requested a print job. *See also* admin alert; error alert.

printer queue A queue that stores print jobs and sends them in turn to a printer or pool of printers.

print operator An operator privilege that allows a user to create, share, and modify printer queues and control print jobs. *See also* accounts operator; server operator.

print processor script A program that is invoked instead of sending a file to a printer.

priority level An attribute assigned to each printer queue that determines which job is processed first when several queues are trying to access the same printer at the same time.

privilege level Under user-level security, one of three settings — user, admin, or guest — assigned for each user account. The privilege level defines the range of actions a user can perform on the network. *See also* guest account, operator privilege, and permissions.

profile A file (used in LAN Manager 2.0 or earlier) containing LAN Manager commands that share resources, establish connections to shared resources, and set printer queue options.

queue *See* printer queue.

redirect To change the default routing or destination of data traffic.

relative path A path relative to the current drive and directory. For example, from the directory *lanman*, a relative path to the directory *lanman/accounts* is simply *accounts*. *See also* absolute path; network path.

remote Used to describe any server or client other than the one at which the user or administrator is currently working. *See also* local.

remote administration Performance of administrative tasks on a server that is not located where the administrator is currently working.

Replicator service A LAN Manager service that maintains identical sets of files and directories on different servers.

resource Any directory, printer, or other equipment that a server can share over a LAN. LAN Manager also has administrative resources, which govern how certain processes work on each server. *See also* disk resource; printer queue; shared resource; sharing.

reset sequence A printer-specific character sequence that invokes or terminates a special function, such as printing in landscape mode.

script *See* logon script; print processor script.

scroll bar A vertical bar that appears at the right of some LAN Manager list boxes, used with the mouse to scroll through a list that contains more information than can be shown in the list box at one time. *See also* scroll box.

scroll box A small square superimposed on a scroll bar in a LAN Manager list box, showing the relative position of the list box in the entire list.

security settings Server options that specify how users can change their passwords and what action the server takes when users violate their logon hours. There are five security settings: minimum password length, minimum password age, maximum password age, password uniqueness, and force logoff. *See also* logon restrictions.

separator page One or more cover sheets that are printed before a print job. Also called a banner page.

serial printer A printer attached to a computer's serial port. *See also* devicename.

server A computer that manages and shares the data and equipment on a LAN.

server operator An operator privilege that allows a user (with user privilege) to start and stop services, share resources, use the server's error log, and close users' sessions. *See also* accounts operator; print operator.

services The main components of the LAN Manager software. The basic service is the Server service, which enables a computer to share network resources. Other services include the Alerter, Netlogon, Netrun, Remoteboot, Replicator, SNMP, Timesource, and UPS services.

session A link between a client and a server. A session consists of one or more connections to shared resources. *See also* connection.

shared resource A resource on a server that has been made available to network users. *See also* resource.

share-level security A security mode that limits access to each shared resource by requiring a password for the resource. Permissions are assigned to the resource, rather than to the user. All users who know the password can use the resource within the bounds of the permissions assigned for it. *See also* user-level security.

sharename The name given to a resource when it is shared on the network. Each shared resource is identified by its sharename, which must be unique on the server that controls the resource. *See also* computername; network path.

sharing Making a server's resources available to network users. *See also* resource.

SNMP Service A LAN Manager service that allows a server to report its current status to a Simple Network Management Protocol (SNMP) or a transport control internet protocol (TCP/IP) network.

standalone logon A logon request that is not validated by a logon server. In a domain not running logon validation, each logon request is processed as a standalone logon. In a domain running logon validation, a logon request from a username not found in the domain's user accounts database is processed as a standalone logon. *See also* logon validation; logon server.

standalone server A server running user-level security that has its own user accounts database and does not participate in logon validation.

statistics A record of server and client activity kept by LAN Manager. Statistics are cleared each time the server or client is turned off, and cannot be saved. Server statistics provide information about how the server is being accessed. Client statistics provide information about how the client is being used.

System Administrative Interface A full screen graphic interface for administering a UNIX system server, run at the UNIX system console.

text box A field in a Net Admin Interface dialog box, used to enter text.

time server The server designated as the network time source with the Timesource service. The time server is the computer with which other computers on the network synchronize.

Timesource service A LAN Manager service that identifies a server as the time source for a domain. Other computers synchronize their clocks with the time server.

UNC (Universal Naming Convention) A convention for identifying shared resources in the format \uname.**`serve`***sharename*, where *uname* is the server's UNIX system name and *sharename* is the home directory's sharename.

uninterruptible power supply *See* UPS.

Universal Naming Convention *See* UNC.

UNIX operating system The multitasking operating system that supports LAN Manager servers.

UPS (uninterruptible power supply) A battery connected to a server's serial port to provide backup power for orderly shutdown in case of failure of the normal power supply.

user account A record on a server or in a domain that identifies an individual network user to LAN Manager.

user accounts database A file kept on servers running user-level security, containing the record of existing network user accounts and groups.

user privilege A privilege that allows a user to use network resources, view information about a server's shared resources and the status of printer queues, and send and receive messages. Users with user privilege belong to the special group *users*. *See also* permissions; privilege level.

user-level security A security mode in which a user account is set up for each user and permissions are assigned to each user for specific resources. The permissions define the actions the user can take with each resource. *See also* logon validation; share-level security.

username Under user-level security, the name by which the network identifies a user. The name is part of a user account, which also includes a password. The username and password are required to access resources shared on a server. Under logon validation, the username and password are required for the user to gain access to the network.

workstation *See* client.

workstation domain The domain of which a client is a member, specified when the Workstation service is started. *See also* logon domain.

Workstation service A LAN Manager service that enables a computer to use network resources and services. The Workstation service must be running for any other service to run.

Index