OS/2 Warp Server for e-business

Network Administrator Tasks

Note

Before using this information and the product it supports, read the general information under “Appendix E. Notices” on page 283.

First Edition

This edition applies to the first edition of OS/2 Warp Server for e-business and to any subsequent releases and modifications until otherwise indicated in new editions.

Contents

Figures

Tables

About This Book

This book contains information about network administration tasks you can accomplish using OS/2 Warp Server for e-business.

The information in this book includes the following:

- Using the graphical user interfaces (GUIs)
- Handling network administrator tasks
- Setting up and backing up a domain
- Managing users and groups
- Sharing network resources with aliases and netnames
- Defining access control profiles
- Limiting directory space accessed by users
- Managing WorkSpace On-Demand, OS/2, DOS, and Microsoft Windows applications
- Printing on the network
- Managing network services, statistics, and audit and error logs
- Managing Local Security on 386 HPFS servers
- Using Fault Tolerance
- Replicating files
- Using remote initial program load (remote IPL)
- Using the Uninterruptible Power Supply (UPS) service
- Using the OS/2 Warp Server or LAN Server directory structure
- Using User Profile Management (UPM) procedures

The appendixes contain information on directory structures and utilities.

Notes:

1. Many administrator tasks can be performed through the command line. Information about network commands is provided in the *Command Reference*.
2. Information on user tasks is provided in the *OS/2 File and Print Client Guide*.
3. Other books contain complementary information. For more information, see “Prerequisite Books” on page xix and “Related Books” on page xix.

For more information about this book, see the following topics:

- “Who Should Use This Book” on page xvi
- “How This Book Is Organized” on page xvi
- “Conventions” on page xvii
- “Online Books and Other Information” on page xix
- “Prerequisite Books” on page xix
- “Related Books” on page xix
- “Note About 386 HPFS” on page xix

Who Should Use This Book

This book is a reference for the OS/2 Warp Server or LAN Server *network administrator*. The network administrator is responsible for installing, managing, controlling, and configuring a network. The network administrator also defines resources to be shared and user access to the shared resources.

Additional users of this book include OS/2 Warp Server users who have been given one or more administrative privileges for a server running OS/2 Warp Server or LAN Server.

Before you begin the tasks in this book, you should plan your network, install the appropriate OS/2 Warp Server or LAN Server components on the clients and servers in your network, and make sure that your DOS workstations have one of the appropriate DOS versions installed. Refer to *Quick Beginnings* for more information.

How This Book Is Organized

This book contains the following chapters and appendixes:

- “Chapter 1. Using OS/2 Warp Server for e-business: Overview” on page 1 provides an overview of the network administrator-only tasks and the graphical user interface (GUI) used to do those tasks. This chapter also discusses getting help from the GUI and the command-line interface.
- “Chapter 2. Setting Up the Domain” on page 5 outlines the steps for setting up your domain and describes setting the time and date, defining servers, backing up the domain control database, and printing the domain definition.
- “Chapter 4. OS/2 Warp Server Personally Safe n Sound (PSnS)” on page 41 describes OS/2 Warp Server Backup/Restore and provides some references for more information.
- “Chapter 5. Managing Users and Groups” on page 43 describes adding, updating, and deleting users and groups from the domain.
- “Chapter 6. Sharing Network Resources” on page 65 describes sharing and managing network resources, including files, printers, and serial devices. This chapter also discusses using aliases and netnames to share resources.
- “Chapter 7. Defining Access Control Profiles” on page 83 discusses the access control system and creating, changing, and deleting user access to resources.
- “Chapter 8. Limiting Space within Directories on 386 HPFS Servers” on page 101 discusses the management of disk space on servers. You can apply limits to a directory tree to control its size and to limit space available to users.
- “Chapter 9. Managing OS/2, DOS, WorkSpace On-Demand, and Windows Applications” on page 113 discusses creating, updating, and deleting shared OS/2 and DOS applications, and preparing for running remote programs.
- “Chapter 10. Managing Windows Applications for DOS LAN Services” on page 127 discusses how to provide network services to users of DOS LAN Services Windows.
- “Chapter 11. Network Printing” on page 131 discusses how to set up and manage network print spooler queues, define separator pages, and attach printers to the network.

- “Chapter 12. Managing the Network” on page 141 describes common network management activities, such as stopping and starting network services, managing serial device queues, and closing open files and active sessions. It discusses auditing, setting server and client parameters, and error logging, and includes a brief description of the network management tool First Failure Support Technology/2 (FFST/2).
- “Chapter 13. Managing Local Security on 386 HPFS” on page 165 discusses Local Security for the 386 HPFS. It provides guidelines and considerations for Local Security.
- “Chapter 14. Using Fault Tolerance” on page 173 describes how to configure and manage the Fault Tolerance system for hard disks. It also discusses error monitoring for the Fault Tolerance system.
- “Chapter 15. Replicating Files” on page 197 describes using the Replicator service to copy files from a server to one or more servers or clients.
- “Chapter 16. Installing and Configuring Remote IPL” on page 207 describes installing Remote IPL with the RIPLINST utility and configuring DHCP Boot.
- “Chapter 17. Managing Remote IPL” on page 227 describes creating, customizing, and deleting remote IPL workstations.
- “Chapter 18. The Uninterruptible Power Supply Service” on page 251 describes support for the Uninterruptible Power Supply (UPS) service.
- “Appendix A. Directory Structure” on page 257 describes the LAN directory structure for clients, servers, and domain controllers.
- “Appendix B. User Profile Management” on page 261 describes the use of User Profile Management to add, update, and delete users and groups from the domain.
- “Appendix C. OS/2 Warp Server Interoperability” on page 273 identifies how the various versions of OS/2 Warp Server, LAN Server, and PCLP work together.
- “Appendix D. DHCP RIPL Bootstrap Messages” on page 281 identifies the Remote IPL error messages (and help for them) supported by ROM BIOS.

This book also contains an index.

Conventions

This book includes several usability aids and conventions to help you find and identify the information you need. The following sections describe these usability aids and conventions:

- “Double-Byte Character Set (DBCS) Information”
- “Notes” on page xviii
- “Attention Notes” on page xviii
- “Highlighting Conventions” on page xviii

Double-Byte Character Set (DBCS) Information

OS/2 Warp Server and LAN Server run on both single-byte character set (SBCS) systems and double-byte character set (DBCS) systems. *SBCS* is a graphic character set in which each character occupies 1 byte. *DBCS* is a graphic character set in which each character occupies 2 bytes. Languages, such as Japanese, Chinese, and Korean, that contain more symbols than can be represented by 256 code combinations require double-byte character sets.

DBCS information is included throughout this book. Restrictions for DBCS systems are indicated by the following:

DBCS Note: The preceding access control profiles do not propagate to DBCS systems.

Notes

Notes provide important information that can affect the operation of the product or the completion of the task, as shown in the following example:

Note: If you later add more users to the group, you must repeat this procedure to add the application for the new users.

Attention Notes

Attention notes indicate situations where you can lose data or damage software or hardware if certain procedures are not followed, as shown in the following example:

Attention: If you have applications running on the Desktop and do not perform a shutdown procedure before you turn off your computer, you may lose data.

Highlighting Conventions

Below are the highlighting conventions used throughout this book and the things they are used to identify:

CAPITAL LETTERS

- Commands
- Directory names
- File names

Bold Controls (when used in procedures), for example:

- Menu bar choices
- Radio buttons
- Push buttons
- List boxes
- Check boxes
- Entry fields
- Read-only text fields

Italics

- Book and diskette titles
- Variable names and values
- Technical terms when introduced
- Words of emphasis

`Monospace`

- Coding examples
- Special characters
- Text reader must type
- Text displayed on the computer screen

Online Books and Other Information

Many OS/2 Warp Server books are shipped in online form with the product. You can view the books from a CD-ROM drive, install them on your hard disk, or view them remotely (if they are installed on a server in the domain). After installation, you can access online books and troubleshooting information from the Assistance Center. See *Quick Beginnings* for a list of OS/2 Warp Server for e-business books.

Note: You can print sections of the online books by using the **Print** function on the menu bar while viewing the books. Also, many books are shipped in PostScript and Adobe format; these can be printed.

Prerequisite Books

Quick Beginnings: Installing OS/2 Warp Server for e-business is a prerequisite for using this book. This book is also referred to as *Installation*.

Related Books

The following books are helpful for the user whose system is connected to a local area network (LAN):

- *OS/2 File and Print Client Guide*
- *DLS and Windows User's Guide*

The following books are also helpful for network administrators:

- OS/2 Warp Server for e-business *Performance Tuning*
- OS/2 Warp Server for e-business *Serviceability and Troubleshooting Guide*
- OS/2 Warp Server for e-business *Command Reference*
- OS/2 Warp Server for e-business *Programming Guide and Reference*
- *MPTS Configuration Guide*

Note About 386 HPFS

In the previous release of OS/2 Warp Server, two different levels of servers (Entry and Advanced) were offered. The Advanced Level Server included both HPFS and 386 HPFS. In this release, 386 HPFS is available if you are upgrading from an Advanced Level Server. However, if you don't already have the Advanced Level Server and you're interested in some of the features offered only through 386 HPFS (such as local security), 386 HPFS is available for an additional fee. See "Chapter 8. Limiting Space within Directories on 386 HPFS Servers" on page 101, "Chapter 13. Managing Local Security on 386 HPFS" on page 165, and "Chapter 14. Using Fault Tolerance" on page 173 to read about some of the features of 386 HPFS.

Chapter 1. Using OS/2 Warp Server for e-business: Overview

This chapter briefly describes the network administrator tasks you can perform using OS/2 Warp Server for e-business and introduces the LAN Server Administration interface.

For more information, see the following topics:

- “Network Administrator Tasks”
- “Graphical User Interfaces and Icons”

Network Administrator Tasks

The following list is an overview of the network administrator tasks:

- Setting up a domain with a domain controller, backup domain controllers, additional servers, and remote IPL servers
- Performing domain controller database (DCDB) backup on your domain controllers
- Adding, deleting, and updating users, groups, and network applications
- Defining access permissions to resources for users and groups
- Starting and stopping the sharing of directories, printers, and serial devices
- Configuring and managing Fault Tolerance for your network
- Setting up remote IPL from a server for a DOS or an OS/2 requester
- Controlling and accessing servers from any server or requester on the network running OS/2 Warp Server.
- Scheduling tasks to run at designated times on a server
- Limiting the directory space available to users
- Viewing the network status and network statistics

Users can perform a subset of these tasks. For information on user tasks, refer to the *OS/2 File and Print Client Guide* or the *DLS and Windows User’s Guide*.

For problem determination tasks, refer to the *Serviceability and Troubleshooting Guide*. For performance tuning tasks, refer to *Performance Tuning*.

You can perform network administrator tasks from either LAN Server Administration or the command-line interface. For information on the command-line commands, refer to the *Command Reference* .

Graphical User Interfaces and Icons

The following list describes each GUI and its functions:

Icon **Function**

Logon: allows you to perform domain logon and local logon (for subsystems requiring local verification). OS/2 Warp Server does not require local logon.

Logoff: allows you to log off the domain. Make sure all network applications are closed before logging off.

LAN Server Administration: allows you to administer a network running OS/2 Warp Server. The interface replaces the full-screen interface used in previous versions of LAN Server. Enhancements from the full-screen interface include the ability to drag and drop some objects, the ability to manage user and group definitions, and the ability to limit directory sizes on users' home directories. National Language Support (NLS) characters entered by using ALT+ *number* on the keyboard cannot be used on notebook pages in this GUI. (This is a Presentation Manager restriction.) Administration of NLS-specific names must be done using a workstation configured for the appropriate language (keyboard and country code).

Audit Log: records OS/2 Warp Server events and user-defined events

Error Log: records OS/2 Warp Server errors, showing the error messages and help text

Tuning Assistant GUI: provides automatic tuning and configuration of your network

Network Messaging GUI: provides the interface for sending and receiving network messages

Network DDE and Clipboard GUI: provides the ability to cut and paste data into other applications on the network using dynamic data exchange (DDE) and Clipboard functions

Installation/Configuration GUI: The OS/2 Warp Server Installation/Configuration program. Use this to reinstall or remove OS/2 Warp Server from the local workstation. You can also create response files (for CID install) from this interface.

Start Server GUI: starts the Server service on the workstation.

MPTS GUI: configures PROTOCOL.INI file parameters for the protocols and NDIS drivers on the workstation. Refer to the online MPTS/2 books in the **LAN Server Books** icon for information about using this MPTS/2 interface.

FFST/2 GUI: provides FFST/2 interface which can be used by other network management products.

Fault Tolerance Setup GUI: provides the FTSETUP utility to set up Fault Tolerance on the network for the first time.

Fault Tolerance Administration GUI: provides the FTADMIN utility to manage Fault Tolerance on the network.

Chapter 2. Setting Up the Domain

Before you can do anything on a network, you must set up one or more *domains.* A domain is a set of servers that allocates shared network resources within a single logical system. After the network is defined, periodically back up the files describing the current domain to minimize loss that can be caused by hard-disk damage.

For more information, see the following topics:

Setting Up the Domain

You can set up your domain only after you have:

- Used the instructions in *Quick Beginnings* or *Quick Beginnings* to complete the installation of OS/2 Warp Server on the domain controller (required), backup domain controllers (optional), and servers (optional), and run the Migration Utility, if necessary.
- Created spooler queues on the appropriate servers through the printer objects. This step is necessary only if you have printers.

The following order is suggested for setting up your domain:

1. (required) Install the software on all servers in the domain.
2. (required) Log on to the domain controller using your administrator user ID and password. If you have not created an administrator user ID, the default ID is USERID and the default password is PASSWORD.
3. Define additional servers on the domain. See “Defining Servers” on page 10.
4. (optional here) Start additional servers.
5. (optional) Because users can log on, disable user logon while you set up the domain by pausing the NetLogon service at the domain controller, either through the LAN Server Administration or by typing:

   ```
   NET PAUSE NetLogon
   ```

See “Managing Network Services” on page 141 for LAN Server Administration instructions or refer to the *Command Reference* for the NET PAUSE description.

6. (required) Define users and groups. See “Chapter 5. Managing Users and Groups” on page 43.
7. (optional) Define shared resources (directories, printers, and serial devices) and their aliases. See “Chapter 6. Sharing Network Resources” on page 65.
8. (required) Define access control profiles for the resources. See “Chapter 7. Defining Access Control Profiles” on page 83.
9. (optional) Install and define public applications to be shared on the appropriate servers. See “Chapter 9. Managing OS/2, DOS, WorkSpace On-Demand, and Windows Applications” on page 113.
10. (optional) Create and define images, and then define remote IPL workstations to the domain. See “Chapter 16. Installing and Configuring Remote IPL” on page 207.
11. (optional) Assign resources to be made available to users during logon (logon assignments). See “Chapter 5. Managing Users and Groups” on page 43.
12. (recommended; required if you did step 4) Establish a plan to back up the domain controller database (DCDB) regularly. See “Backing Up and Restoring the Domain Control Database” on page 19.
13. If user logon was disabled at step 5, enable the logon by typing:

    ```
    NET CONTINUE SERVER
    ```
14. (recommended) Print your domain definition for archival purposes. See “Displaying and Printing the Domain Definition” on page 17.

Starting the Domain Controller

The *domain controller* is the primary server in a domain.

The Server service is started automatically unless you specify otherwise. If during installation you did not choose to start the Server service automatically, you can start it by opening **Start Server**. You can also start it by typing `NET START SERVER` at the command line.

Starting OS/2 Warp Server on Your Workstation

You must start the domain controller to allow users to log on to the domain. The users at the requester workstations cannot access LAN resources unless the domain controller and associated servers are running. OS/2 Warp Server is configured to start automatically when the workstation starts.

To start OS/2 Warp Server on a workstation:

1. Open **Start Server** or **Start Requester**.

You can also start OS/2 Warp Server by using the NET START command at the OS/2 command prompt. For the NET START syntax, see the *Command Reference*.

Stopping OS/2 Warp Server on Your Workstation

You can stop individual services on your workstation or you can stop OS/2 Warp Server. For information about stopping individual services, such as the Peer service, refer to “Guidelines for Stopping and Pausing Network Services” on page 143.

When you stop OS/2 Warp Server, other users cannot access the resources on your workstation. If you do not want to stop sharing your resources, do not stop OS/2 Warp Server. If you are preparing to leave work for the day, you can simply lock up your workstation instead of stopping OS/2 Warp Server or shutting down and turning off your workstation. For more information about Lockup, refer to the *OS/2 Desktop Guide* .

Before you stop OS/2 Warp Server, check to see if anyone is connected to your resources. Notify these people that you are going to stop OS/2 Warp Server so that they can finish working with the resources before they are disconnected. You can use Network Messaging to send a message to all users who have open files or active sessions to tell them you are going to stop OS/2 Warp Server on your workstation.

To stop OS/2 Warp Server:

1. Open **LAN Server Administration**.
2. Select **OK** at the IBM logo screen and log on if prompted to do so.
3. Open **Local Workstation**.
4. Open **Services**.
5. Select the **Server service**.
6. Press mouse button 2 to display the menu.
7. Select **Stop**.

Note: If you are going to turn off your workstation or restart it, you first must select **Shut down** from the Desktop. For more information about Shut down, refer to the *OS/2 Desktop Guide* .

You can also stop OS/2 Warp Server by using the NET STOP command at the command line. For the NET STOP syntax, see the *Command Reference* .

Logging On

Logging on identifies you to the local workstation and allows you to gain access to resources on the network. If you are not logged on, you cannot connect to shared resources on your network.

Note: Use the User ID and password that you created during installation of OS/2 Warp Server the first time you log on.

To log on:

1. Open **Logon**. The OS/2 Warp Server Logon window is displayed.
2. In the **User ID** field, type your user ID and press Tab.
3. In the **Password** field, type your password if you have one. If a password is required and you do not supply it, you receive an error message. The password is not displayed on the screen as you type it.
4. If you want to log on to a domain other than the domain listed in the **Domain** field, type the new domain name in the **Domain** field.
5. Select **OK**.

You can also log on by using the LOGON command at the OS/2 command prompt. For the LOGON syntax, see the *Command Reference*.

Logging Off

Logging off disconnects you from resources on the network and prevents you from making new connections to resources. Logging off OS/2 Warp Server does not stop OS/2 Warp Server on your workstation. If your workstation is a server or peer workstation, other users can continue to access your shared resources until you stop the Peer service (peer workstation only), stop sharing the resources, or turn off your workstation.

Note: If you are running any network applications when you log off, OS/2 Warp Server prompts you to determine if you want to stop the applications. If you do not want to stop the applications, your logoff request is canceled.

To log off:

1. Open **Logoff**.
2. A window is displayed that lists all of the sessions to which you are currently logged on. You can select each local OS/2 session to be logged off or select **Log off All** to log off all active sessions.

   If you are logged on only to an OS/2 Warp Server or LAN Server domain, you probably have only one session displayed to log off. If you have logged on to database manager in addition to logging on to OS/2 Warp Server, you have multiple sessions to log off.

Note:

If you are going to turn off your workstation or restart it, you must first select **Shut down** from the Desktop. For more information about Shut down, refer to the *OS/2 Desktop Guide*.

Do not shut down your workstation if other users are connected to your resources. Shutting down your workstation stops all active sessions. If you are leaving your workstation, you can use the Lockup utility rather than shut down. Lockup locks your keyboard and mouse until you enter your keyboard password. While Lockup is in effect, all of your sessions can continue to run. For more information about Lockup, refer to the *OS/2 Desktop Guide*.

You can also log off by using the LOGOFF command at the command line. For the LOGOFF syntax, see the *Command Reference*.

Starting and Stopping LAN Server Administration

You must start the domain controller to allow other servers to start and to allow users to log on to the domain. The users at the requester workstations cannot access LAN resources unless the domain controller and associated servers are running. Refer to “Starting OS/2 Warp Server on Your Workstation” on page 6 for more information.

To start LAN Server Administration:

1. Open **LAN Server Administration**.
2. Select **OK** at the IBM logo screen and log on if prompted to do so.

You can also use the NETGUI command to start the GUI. Enter the following at an OS/2 command prompt:

```
NETGUI
```

Refer to “Stopping OS/2 Warp Server on Your Workstation” on page 7 for information about stopping the GUI.

Defining Servers

When you install OS/2 Warp Server or LAN Server on a workstation and define that workstation as the domain controller, that domain controller is the only workstation defined to the domain. You must then define any other servers to belong to this domain.

Servers own resources and respond to requests from users on the network to use those resources. A server definition includes the server machine ID, a brief description of the server, and the domain to which the server belongs.

Peer workstations are requesters that share their resources with requesters and other servers on the LAN. In this respect, peer workstations function as a limited type of server. Peer workstations are not defined to the domain controller. They can be administered locally using the Shared Resources and Network Connections notebook and the Network User Account notebook (for more information, see the *OS/2 File and Print Client Guide*). They can be administered remotely using the command line (for more information, see the *Command Reference*).

When you define additional servers to the domain, make sure that all requesters are configured with enough NetBIOS sessions to allow session establishment with all servers in the domain. Refer to *Quick Beginnings* for more information on configuring NetBIOS parameters.

When you define a workstation as an additional server, the system automatically creates a user ID identical to the server machine ID and places it in the SERVERS group. The descriptive text for this ID is `System ID – Server`. If you delete this user ID, you remove that server from the domain.

System-generated IDs are treated as any other user IDs defined to the domain. User Profile Management, OS/2 Warp Server, and LAN Server windows display system-generated IDs as user IDs. System IDs for additional servers are automatically placed in the group named SERVERS.

Do not delete access control profiles or change access permissions assigned to the system-generated IDs.

User definitions are stored in a file called NET.ACC. Users have a single user definition on the multiple servers in a domain. OS/2 Warp Server and LAN Server provide this capability by keeping the copies of the NET.ACC file in synchronization with each other. The master copy of the NET.ACC file is kept on the domain controller, and copies of it are on the additional servers. The NetLogon service keeps all the NET.ACC user definitions in the files in synchronization. The NET.ACC file determines which file is the master and which is a copy. The primary role indicates the master copy, and all other roles except the stand-alone role indicate a copy.

For more information, see the following topics:

- “Defining Server Roles in a Domain”
- “Domain Logons” on page 12
- “Multiple Logons” on page 13
- “Logging a Domain Controller onto Another Domain” on page 13
- “Backing Up the NET.ACC File” on page 13
- “Initializing the NET.ACC File” on page 13
- “Creating Server Definitions” on page 14
- “Updating Server Definitions” on page 15
- “Deleting Server Definitions” on page 16
- “Implementing Support for Multiple Server Names” on page 16

Defining Server Roles in a Domain

Servers in a domain must run the NetLogon service to keep the server’s copy of the user definitions in synchronization with the domain controller. The NetLogon service is installed with OS/2 Warp Server or LAN Server. Each server has a defined role, and each role causes the NetLogon service to treat the server differently. The roles are as follows:

- *Primary* (domain controller) – This server is specified as the domain controller when OS/2 Warp Server or LAN Server is installed.

  Note: To change the role of an additional server or backup domain controller to Primary, you must reinstall the server as a domain controller.

  Only one server per domain can be the primary domain controller. The domain controller handles network logon requests and contains the master file that holds the user and group definitions. Updates to this file are made at the domain controller and then copied to all servers on the domain.

- *Member* (additional server) – These servers are specified as additional servers when OS/2 Warp Server or LAN Server is installed.

  Multiple member servers can be defined on a domain. Each receives a copy of the user and group definitions file from the domain controller when updates are made. Members cannot handle network logon requests, but they can provide users the resources for logon assignments and applications.
- *Backup* (backup domain controllers) – Servers in a domain can be defined as backup domain controllers.

  Multiple backup domain controllers can be defined on a domain. Each receives a copy of the user and group definitions file from the domain controller when updates are made. If the DCDB Replicator service is running, a full copy of the DCDB is replicated on each. Backup domain controllers can handle network logon requests.

  If the primary domain controller fails, the backup domain controller does not automatically take the primary role, but it handles command-line and OS/2 Warp Server Administration logon requests. If the domain controller fails and the backup domain controller serves logon requests, all resources with aliases should still be available, except those on the domain controller.
- *Stand-alone server* – A stand-alone server is a server that is not defined as part of a domain.

  Workstations that are configured to run the Peer service also have the *Role of server* field set to *Stand-alone*. A workstation designated as a stand-alone server does not respond to logon authorization requests.

You can change a server's role with the NET ACCOUNTS command. For more information about the NET ACCOUNTS command, see the *Command Reference* .

Additional installation and configuration can be required to complete a role change. For example, if you want to change an additional server to a domain controller or backup domain controller, use the OS/2 Warp Server installation program to change the configuration of the additional server into one for a domain controller or backup domain controller. The installation program installs a new DCDB at the additional server.

Domain Logons

Domain logons are handled by a server whose domain role is either backup or domain controller. As a backup domain controller, this type of server can validate user logon assignments and alias resolution like a domain controller.

Whether the domain controller or the backup server handles a network logon request is determined by the value specified in the logon server field in the user account information. If the logon-server value specified is `any` (default), the first backup or domain controller server that answers the user request for logon handles the logon.

The first server that answers can be influenced by relative position on the network with regard to the workstation or speed of the processor on the server. If the domain controller is the preferred server to validate logons, issue the NET USER command with the value of the **logonserver** parameter set to `NULL`. The `NULL` value causes the domain controller to handle the domain logon requests unless busy or unavailable. If the domain controller is busy or unavailable, any backup server in the domain handles logons. For information on how to change this value, see the *Command Reference*.

Multiple Logons

A single user ID can log on to multiple requesters at a time. Use the same user ID and the same password on the same site token ring. You can log on multiple times to access resources available to you. You can log on to every machine in the domain including the domain controller without logging off of any machine. This capability is enabled by default.

Logging a Domain Controller onto Another Domain

If an administrator logs a domain controller onto another domain, a user with Administrator authority can remotely issue NET ADMIN commands that will affect the other domain, rather than the logon domain.

Thus, to prevent unexpected side effects and for security reasons, do not leave servers logged on to other domains with Administrator authority.

Backing Up the NET.ACC File

If you have not made a backup copy of the NET.ACC file *on each server* in C:\IBMLAN\ACCOUNTS, do so now. For more information, refer to “Using the BACKACC Utility to Back Up the NET.ACC File” on page 20. The NET.ACC file contains information that is different for each server and that is not copied using the NetLogon service. (The NetLogon service copies only user and group definitions.)

If the NET.ACC file is lost or damaged on a server, do the following:

1. Configure so that OS/2 Warp Server does not start at reboot. Copy the backup NET.ACC file (unique to that server) to the server. This copy contains necessary workstation-unique information.
2. Start the server again on the LAN. Because the server is running the NetLogon service, the domain controller copies its NET.ACC file to the server. This operation copies the user and group definitions back into the file.

Note: If the passwords become unsynchronized, refer to “Resynchronizing Passwords with the NetLogon Service” on page 30.

For more information on the NetLogon service parameters, refer to *Performance Tuning*. For more information on backing up the NET.ACC file, see “Backing Up and Restoring the Domain Control Database” on page 19.

Initializing the NET.ACC File

The following procedure describes how to initialize the NET.ACC file. You might need to do this if a new NET.ACC file is installed on an additional server or if the NetLogon Service fails to start.

At the server with the new NET.ACC file or where the NetLogon Service is failing, log on as an administrator and perform the following steps.

To initialize the NET.ACC file:

1. Make a note of the current role of the server.
2. Temporarily change the role of the server to PRIMARY with the following command:

```
NET ACCOUNTS /ROLE:PRIMARY
```

3. Add the group account SERVERS to the accounts database (NET.ACC) with the following command:

   ```
   NET GROUP SERVERS /ADD
   ```

4. Add the server as a user account in the accounts database with the following command:

   ```
   NET USER servername /ADD /PRIV:USER /ACTIVE:NO /EXPIRES:NEVER /PASSWORDREQ:NO
   ```

5. If the server is to be the domain controller (PRIMARY), perform the following steps:

   a. Set the server’s account password to NULL with the following command:

      ```
      NET USER servername ""
      ```

      where *servername* is the name of your server.

   b. Add the GUEST ID to the accounts database with the following command:

      ```
      NET USER GUEST /ADD /PRIV:GUEST /PASSWORDREQ:NO
      ```

6. Add the server to the SERVERS group in the accounts database with the following command:

   ```
   NET GROUP SERVERS servername /ADD
   ```

   where *servername* is the name of your server.

7. Restore the server’s original role with one of the following commands:

   ```
   NET ACCOUNTS /ROLE:MEMBER
   ```

   or

   ```
   NET ACCOUNTS /ROLE:BACKUP
   ```

Creating Server Definitions

The procedures to define a server to the domain are different for OS/2 servers and Microsoft Windows NT servers. Use the appropriate procedure from below.

To create a definition for an OS/2 server:

1. Open **LAN Server Administration**.
2. Open the appropriate domain object.
3. Open **Defined Servers**.
4. Drag the **Server Template** to an open area in the Defined Servers folder.

   The Defined Server - Create notebook is displayed.
5. Complete the Identity page.
6. Select **Create**.

To create a definition for a Microsoft Windows NT server:

Adding a Windows NT server to the OS/2 Warp Server domain is a two-step process. You must first install the IBM Networks User Account Manager service on the Windows NT server and then define the NT server as an additional server on the OS/2 Warp Server domain.

1. **To install the IBM Networks User Account Manager service on the Windows NT server:**

   a. Click on **Start**, point to **Settings**, and select **Control Panel**.

   b. Open **Network**.

c. Click on the **Services** tab, and then click on **Add**.

   The Network notebook is displayed.

d. Click on **Have Disk** and insert the OS/2 Warp Server CD-ROM.

e. Type the directory path to the IBM Networks User Account Manager installation files, then click on **Ok**.

   The OEM option window is displayed.

   Note: You can install the IBM Networks User Account Manager from a local or shared network drive (for example, a:\ or d:\IBMINT), from a UNC network path (for example, \\DEPT_SREVER\IBMNT), or from the OS/2 Warp Server CD-ROM.

f. Click on **IBM Networks User Account Manager** and then on **Ok** to copy the files. After this is complete, the Properties notebook is displayed.

g. In the Persistent Users box add the names of persistent users.

h. In the Persistent Localgroups box add the names of persistent localgroup aliases.

   Note: Persistent Users and Localgroups are those managed solely by the Windows NT server and are not synchronized by the OS/2 Warp Server domain controller.

i. Click on **Ok**.

   The Network notebook is displayed.

j. Click on the **Identification** tab and then click on **Change**.

k. Select **Workgroup** and type the name of the OS/2 Warp Server domain.

l. Click on **Ok** and then on **Close**.

m. On the Network Setting Change window, click on **Yes** to restart your Windows NT system.

2. **To define the Windows NT server in the OS/2 Warp Server domain:**

   Define the Windows NT server in the same manner as an OS/2 server. See **To create a definition for an OS/2 server** for the procedure.

Updating Server Definitions

You can update server definitions.

To update a server definition:

1. Open **LAN Server Administration**.
2. Open the appropriate domain object.
3. Open **Defined Servers**.
4. With mouse button 2, select the appropriate server object.
5. Select **Properties**.

   The notebook of the selected server is displayed.
6. Check all the properties for each page, and update the definitions to meet your needs.
7. Select **Set** or **Apply**.
8. Select **Object**.

   The following menu selections contain additional properties or displays:

   - Selections that you can view, modify, or refresh
     – **Open files**

   - **Active sessions**
- Selections that you can view, refresh, clear, or print
   - **Statistics** (for servers and requesters)
- Selection that you can view, share, change, refresh, and manage
   - **Current shares**
- Selection that you can add, change, or delete
   - **Current assignments**

9. Select these items one at a time, and view or change the properties as required.
10. Select **Close**.

Deleting Server Definitions

Before deleting a server definition, you should first delete any aliases and home directories associated with the server. For more information on deleting aliases, see “Determining the Server on Which a Resource Resides” on page 74 and “Deleting an Alias” on page 73.

Again the procedures for deleting a server definition are different for OS/2 servers and Windows NT servers. Use the appropriate procedure from below.

To delete an OS/2 server definition from the domain:

1. Open **LAN Server Administration**.
2. Open the appropriate domain object.
3. Open **Defined Servers**.
4. Select the server object that you want to delete.
5. Press mouse button 2, and select **Delete** from the pop-up menu.

To delete a Windows NT server definition from the domain:

1. **Delete the IBM Networks User Account Manager Service from the Windows NT server:**
   a. Click on **Start**, point to **Settings**, and select **Control Panel**.
   b. Open **Network** and select **Services**.
   c. Select IBM Networks User Account from the Network Services list.
   d. Select **Remove** and click on **Yes**.
   e. Click on **Close**.
   f. Restart your system.
2. **Delete the Windows NT server definition from the domain.**

   Delete the NT server in the same manner as an OS/2 server. See **To delete an OS/2 server definition from the domain** for the procedure.

   Attention: Deleting the server definition is critical, even if you are planning on immediately re-installing the IBM Networks User Account Manager service. Failing to delete the server definition causes the domain controller and the Windows NT server to be out of synch.

Implementing Support for Multiple Server Names

OS/2 Warp Server supports multiple server names. The machine name located in the server’s IBMLAN.INI COMPUTERNAME= field is considered the primary server name. Additional server names, also known as secondary names, can be added to allow a server to respond to and service requests for these servers.

The ability to support multiple server names allows the following:

- Merging or migrating servers from older hardware to faster, more powerful server hardware without reconfiguring aliases or server names in the domain
- Temporarily offering resources (such as printer shares) for a server that is unavailable, because of failure or maintenance
- Support for products that might require the feature for supporting automatic server failover

There are many options available for adding and managing secondary server names:

- Through the Network API (see NetServerNameAdd and NetServerDel in the *OS/2 Programming Guide and Reference Addendum*)
- Through the command line (see NET CONFIG SERVER /OTHSRVNAMES in the *Command Reference*)
- Through the OTHSRVNAMES= parameter in the IBMLAN.INI
- Through the /OTHSRVNAMES option to NET START SERVER (see the *Command Reference*)

Example: Setting one printer server to temporarily replace another

In this example, PRTSRV9 is scheduled for hardware maintenance, so PRTSRV7 will be switched to cover printing requests for PRTSRV9. To do this, you must switch the printers and create queues.

1. At the command line, type

   ```
   NET CONFIG SERVER /OTHSRVNAMES:PRTSRV9
   ```

2. To switch the printers, physically switch the printer cable from one server to another.
3. To create the printer queue, use the printer template and create a new queue with the same properties as the original queue.
4. Restart the printer shares by typing

   ```
   NET STOP LSSERVER
   NET START LSSERVER
   ```

Displaying and Printing the Domain Definition

Using LAN Server Administration, you can display the domain definition or print it for reference or record-keeping purposes. The domain definition has the following sections:

- Users
- Groups
- Aliases
- Public Applications
- Defined Servers

You can also use the NET ADMIN command to run the DSPDOMDF utility, which displays and prints domain-related information. Run the DSPDOMDF utility at a primary or backup server because this utility uses account information from the local accounts database (NET.ACC).

For more information, see the following topics:

- “Displaying Server Information”
- “Printing Domain Information”

Displaying Server Information

You can display information about a remote server using the OS/2 Warp Server Administration.

To display information about a remote server:

1. Open **LAN Server Administration**.
2. Open the appropriate domain object.
3. Open **Defined Servers**.
4. With mouse button 2, select the appropriate server object.
5. Select **Properties**.

   The notebook of the selected server is displayed.
6. Review all the pages as desired for information about this server.

You can also display information about a remote server by typing:

```
NET ADMIN \\rmtsrv /C "DSPDOMDF"
```

where *rmtsrv* is your remote server.

Printing Domain Information

Use the following procedure to print out information about domain definitions. You must perform this procedure on a local server defined in the domain for which you are printing the information.

To print domain definitions:

1. Open **LAN Server Administration**.
2. With mouse button 2, select the appropriate domain object
3. From the pop-up menu, select **Print definitions**.

   The domain definition is printed on the local printer.

You can also print domain information by redirecting the output of the NET ADMIN command to a file or a device by typing:

```
NET ADMIN \\rmtsrv /C "DSPDOMDF"
```

where *rmtsrv* is your remote server and then typing:

```
DSPDOMDF > lpt1
```

where *lpt1* is the file or device, such as a printer.

Time and Date Considerations

During server startup, the date and time on the server are synchronized with the date and time on the domain controller. With the Timesource service, you can designate a server as a reliable source of the time and date for synchronization of other workstations in the domain.

For more information, see the following topics:

- “Designating a Server as a Date and Time Source”
- “Setting the Date and Time”

Designating a Server as a Date and Time Source

Use the following procedure to identify a server as the source for time and date across a domain.

To designate a server as a date and time source:

1. Open **LAN Server Administration**.
2. Open the appropriate domain object.
3. Open **Defined Servers**.
4. Open the appropriate server object.
5. Open **Services**.

   The details view of the Services container is displayed so that you can view the current status of all installed services.
6. If you want to view the properties of the Timesource service, open its icon.
7. After you have viewed the properties, close the notebook.
8. With mouse button 2, select **Timesource Service**.
9. From the pop-up menu, select **Start**.

   The Start Service window is displayed.
10. Select **Start**.

Setting the Date and Time

You can set the time and date on the domain controller from a server or any requester by using the NET TIME command. Changes are passed automatically to all servers in the domain. Requester clocks are updated when the next user logs on. Date and time changes stay in effect until you start your workstation again. For example, to set the date on DOMAIN1 to September 23, 1995, and the time to 19:30, type:

```
NET TIME /DATE:09-23-95 /TIME:19:30 /DOMAIN:DOMAIN1
```

For more information about the NET TIME command, refer to the *Command Reference* .

Backing Up and Restoring the Domain Control Database

The *domain controller database* (DCDB) resides in the \IBMLAN\DCDB directory on the domain controller. The DCDB contains files that describe the current domain. For more information on the structure and contents of the \IBMLAN\DCDB directory, see “Appendix A. Directory Structure” on page 257.

The following information describes suggested procedures to:

- Back up the OS/2 Warp Server domain controller database, including the NET.ACC file.
- Configure an additional server as the temporary domain controller after failure of the original domain controller.
- Restore the domain definitions from the temporary domain controller to the original domain controller.

These backup and restore procedures apply only to the domain definitions contained in the domain controller database subdirectory (the information listed in “Displaying and Printing the Domain Definition” on page 17). These procedures assume that other procedures are used, as required, to back up and restore application files and user data files. In the event of domain controller failure, restore the required application files and data files before restoring the domain controller database.

The following pages describe these two scenarios:

- Using the DCDB Replicator service (DCDBREPL) on the domain controller and a backup domain controller to back up and restore the \IBMLAN\DCDB directory tree, and the BACKACC and RESTACC utilities to back up and restore the access control profiles. The domain controller and backup domain controller are defined during the OS/2 Warp Server or LAN Server installation/configuration program.
- Using the XCOPY command and the OS/2 Warp Server AT command to back up and restore the appropriate files. This action involves a domain controller and an additional server.

These two scenarios assume that:

- The NetLogon service is started at server startup.
- The domain controller machine ID is DCSERV.
- The administrator ID LANBKID is set up so that when the ID is logged on, the Z drive is assigned to the directory above the IBMLAN subdirectory on the additional server.

For more information, see the following topics:

- “Using the BACKACC Utility to Back Up the NET.ACC File”
- “Using the DCDB Replicator Service to Back Up the DCDB” on page 21
- “Copying Files to Back Up the DCDB” on page 23
- “Activating the Backup Domain Controller” on page 24
- “Recovering After Domain Controller Failure” on page 24
- “Restoring Files to the Original Domain Controller” on page 25
- “Allowing Adequate NET.ACC Synchronization Time” on page 28

Using the BACKACC Utility to Back Up the NET.ACC File

Note:

> In order to run the BACKACC utility on a machine installed with Local Security, you must:
>
> - Be logged on locally as an administrator

- Have access to the \IBMLAN\ACCOUNTS subdirectory
- Have access to the root directory of your current drive

For a complete backup of the DCDB, you must back up the NET.ACC file and any access control profiles associated with 386 HPFS drives. (The NET.ACC file contains user and group information and access control profiles.) The NetLogon service automatically copies the user and group information to all servers in the domain. The NET.ACC file also contains server-specific access control information for file allocation table (FAT) drives, pipes, printers, and serial devices that is not copied to the other servers in the domain. (The 386 HPFS drive store their access control profiles as an integral part of their file systems.) These access control profiles are unique to each server. The NET.ACC file is kept open by the server and cannot be copied while the server is running.

Because the NET.ACC file cannot be copied, you must use the BACKACC utility to back up the NET.ACC file and the access control information for both 386 HPFS and FAT drives. The RESTACC utility restores the access control information for the drives. Restore the NET.ACC file by using the procedure on page “Restoring Files to the Original Domain Controller” on page 25.

You can create a backup of the NET.ACC file at each startup to protect the user and group IDs defined within User Profile Management. To create a backup at startup, add the following statement to the STARTUP.CMD file:

```
BACKACC /S
```

This command saves a copy of the current NET.ACC file at the next system startup.

Note: The BACKACC utility does not require you to stop the server.

You can use the AT command to schedule periodic backups. For example, for FAT drives:

```
AT 23:00 /E:M,W,F BACKACC
```

For 386 HPFS drives:

```
AT 23:00 /E:M,W,F BACKACC C:\ /A /S
```

If you want to back up multiple drives, issue the BACKACC command specifying the drive letter for each drive. See *Command Reference* for more information about using the BACKACC utility.

Using the DCDB Replicator Service to Back Up the DCDB

The following process sets up the DCDB Replicator service on the domain controller and the backup domain controller. DCDB Replicator service parameters are described in *Performance Tuning*.

If large files that change frequently are replicated often (that is, the **interval**, **pulse**, and **guardtime** parameter values are low), then the number of file I/O operations can decrease performance. You can improve this possible decrease in performance if you replicate the files less frequently (that is, increase the **interval** and **pulse** parameter values).

This scenario uses a special version of the Replicator service—the DCDB Replicator service—to back up the files in the DCDB subdirectory. Parameters that would have to be set manually to perform this task using the Replicator service are automatically set by the DCDB Replicator service. These parameter settings free the Replicator service for other tasks.

To set up the DCDB Replicator service to back up the DCDB subdirectory tree:

1. On the domain controller, create the REPL.INI file in each first-level subdirectory of the IBMLAN\DCDB directory with the following contents:

   ```
   extent = tree
   integrity = file
   ```

2. To maintain IPL images at the domain controller and have the copies at the additional servers updated periodically, do not create (or remove, if already created) the USERLOCK. *xxx* file. The DCDB Replicator service automatically excludes the IMAGES subdirectory. (The USERLOCK. *xxx* file works only in a first-level subdirectory beyond the export path and only if the **integrity** parameter value equals `TREE`.)

   Note: If the Remote IPL service is installed on the backup domain controller, the IMAGES subdirectory is not replicated from the domain controller. The NO_SYNC.RP$ file is placed in the IMAGES subdirectory. See “Chapter 15. Replicating Files” on page 197 more information about this file.

3. Make sure that the DCDB Replicator section (DCDBREPL) of the IBMLAN.INI file of the domain controller includes the following settings:

   ```
   interval = 5
   guardtime = 2
   pulse = 3
   random = 60
   ```

4. Add DCDBREPL to the **srvservices** parameter as another service to be started at server startup, if it is not already there.
5. Make sure that the DCDB Replicator (DCDBREPL) section of the IBMLAN.INI file of the backup domain controller includes the following:

   ```
   tryuser = yes
   logon = userid
   password = password
   ```

   The *userid* and *password* must belong to a user with administrator authority for the DCDB Replicator service to function when no one is logged on to the backup domain controller. Administrator authority is required for the backup domain controller to read DCDB information on the domain controller.
6. Add DCDBREPL to the **srvservices** parameter as another service to be started at server startup on domain controllers and backup domain controllers, if it is not already there.
7. The DCDB Replicator service is automatically installed on domain controllers and backupdomain controllers. For an additional server, you must install the DCDB Replicator service.
8. Make sure the following subdirectories exist on the backupdomain controller:

   ```
   C:\IBMLAN\DCDB\USERS
   C:\IBMLAN\DCDB\DEVICES
   C:\IBMLAN\DCDB\PRINTERS
   C:\IBMLAN\DCDB\APPS
   C:\IBMLAN\DCDB\FILES
   C:\IBMLAN\DCDB\LISTS
   C:\IBMLAN\DCDB\DATA
   ```

If OS/2 Warp Server is installed on a drive other than drive C, these paths should reflect the drive where OS/2 Warp Server is installed.

9. The DCDB Replicator service starts either when the servers are started or when the service is explicitly started on both the domain controller and the backup domain controller. To begin replication of files, start the DCDB Replicator (DCDBREPL) service from an OS/2 command prompt with a NET START DCDBREPL command at both servers.

   If the service is already started, replication does not occur. To begin replicating, you must first stop and then restart the service from an OS/2 command prompt by typing:

   ```
   NET STOP DCDBREPL
   NET START DCDBREPL
   ```

Copying Files to Back Up the DCDB

The following process is an alternative to using the DCDB Replicator service. It results in running a command file that copies files from the domain controller to an additional server on a scheduled basis.

The command file does the following:

1. Logs on an administrator ID (LANBKID). A logon assignment of drive Z is made for LANBKID to the root directory of the additional server.
2. Issues XCOPY commands to copy the required files.
3. Logs off the administrator ID.

Because the administrator ID and password are part of the command file, you must update the password in the command file. Place the command file in a secure directory (that is, a directory that is not accessible by other user IDs). For performance reasons, schedule this command file to run at times of low network use.

To set up a command file:

1. At the domain controller, create a command file containing the following commands. In this example, the file is BACKIT.CMD, and it is stored in the NETPROG subdirectory.

   ```
   C:\MUGLIB\LOGON LANBKID /P:password
   C:\OS2\XCOPY C:\IBMLAN\DCDB\USERS Z:\IBMLAN\DCDB\USERS /S /E
   C:\OS2\XCOPY C:\IBMLAN\DCDB\DEVICES Z:\IBMLAN\DCDB\DEVICES /S /E
   C:\OS2\XCOPY C:\IBMLAN\DCDB\PRINTERS Z:\IBMLAN\DCDB\PRINTERS /S /E
   C:\OS2\XCOPY C:\IBMLAN\DCDB\APPS Z:\IBMLAN\DCDB\APPS /S /E
   C:\OS2\XCOPY C:\IBMLAN\DCDB\FILES Z:\IBMLAN\DCDB\FILES /S /E
   C:\OS2\XCOPY C:\IBMLAN\DCDB\LISTS Z:\IBMLAN\DCDB\LISTS /S /E
   C:\OS2\XCOPY C:\IBMLAN\DCDB\DATA Z:\IBMLAN\DCDB\DATA /S /E
   C:\MUGLIB\LOGOFF
   ```

   Note: The `/S` parameter copies nonempty subdirectories within the path; `/E` copies empty subdirectories with the `/S` parameter. If the OS/2 program or subdirectory \MUGLIB is installed on a drive other than C, these paths should reflect the drive where those products are installed.

2. Schedule the running of this command file using the OS/2 Warp Server AT command. This command may be included in a command file. For more information and the syntax of the AT command, refer to the*Command Reference*.

   For example, type:

   ```
   AT 01:00 /E:M,T,W,TH,F  C:\IBMLAN\NETPROG\BACKIT
   ```

This example command copies the files at 1 a.m., Monday through Friday.

Note: You can specify only one time value at a time with the AT command. For example, you could not specify both 01:00 and 12:00.

The files in the specified DCDB subdirectories are copied to the additional server at the time specified by the AT command. No user is likely to be logged on at the scheduled backup time. The Replicator service is available to replicate other files on the domain controller.

Activating the Backup Domain Controller

If you have not properly activated your backup domain controller, your users may get errors when logging on, or your domain control database (DCDB) may not be properly replicated to the backup domain controller. To activate the backup domain controller, complete these steps:

1. Define a user ID at the domain controller with the correct authorizations and log onto the domain controller at the backup domain controller with that user ID. For example, a user ID with administrator authority would allow DCDB replication at the backup domain controller.

   Read (R) and Attribute (A) access permissions are required to replicate the data under the DCDB directory. Refer to “Chapter 7. Defining Access Control Profiles” on page 83 for more information regarding specific authorizations to support DCDB replication.

2. Start the DCDBREPL service on both the domain controller and the backup domain controller.

   The DCDBREPL service is started automatically on the backup domain controller and must be selected to start on the domain controller. The backup domain controller is not activated until DCDBREPL is started on the domain controller. To start the DCDBREPL service at the domain controller, complete one of the following steps:

   - Select the **DCDB Replicator on** install option on the Server Services panel.
   - Start the DCDBREPL service automatically when the server is started by adding DCDBREPL to the SRVSERVICES line in IBMLAN.INI; for example:

     ```
     SRVSERVICES = NetLogon,LSSERVER,DCDBREPL
     ```
   - Add the following to STARTUP.CMD:

     ```
     NET START DCDBREPL
     ```
   - Start the DCDBREPL service with the following command:

     ```
     NET START DCDBREPL
     ```

Recovering After Domain Controller Failure

The following procedure configures an additional server as the temporary domain controller after the original domain controller fails. If your domain controller fails and you have a backup domain controller, your domain continues to operate properly, except for resources on the domain controller itself and some logon assignments such as home directories. If the primary domain controller must be down for an extended period, you can change the role of the backup to primary. This change allows users to get their logon assignments and the administrator to define new aliases or users.

To configure an additional server as a domain controller:

1. Stop the NetLogon service at the additional server, either from the OS/2 Warp Server Administration or at the command line. At the command prompt, type:

   ```
   NET STOP NetLogon
   ```
2. Change the role of the additional server to Primary, so it can serve as a temporary domain controller. At the command prompt, type:

   ```
   NET ACCOUNTS /ROLE:PRIMARY
   ```
3. Restart the NetLogon service at the additional server. At the command prompt, type:

   ```
   NET START NetLogon
   ```

   Until the role is explicitly changed by another NET ACCOUNTS command, this server automatically starts up as the domain controller.

   Note:

   > If the service is already started, replication does not occur. To begin replicating, you must first stop and then restart the service from an OS/2 command prompt by typing:
   >
   > ```
   > NET STOP DCDBREPL
   > NET START DCDBREPL
   > ```
   >
   > The following step is not necessary if the DCDB Replicator service backed up the DCDB.
4. When the server starts, it creates the proper access control profiles needed for the subdirectories in the \IBMLAN\DCDB directory, unless the access control profiles already exist. However, the server does not create access control profiles for individual user directories (\IBMLAN\DCDB\USERS\ *userid*).

   Using LAN Server Administration, create access control profiles for each user directory (\IBMLAN\DCDB\USERS\ *userid*). Give users full access (RWCXDAP) to their user directories. For more information about creating access control profiles, see “Creating an Access Control Profile” on page 90.

Users can log on to the domain but cannot access resources (printers, files, applications, serial devices, and home directories) on the original domain controller.

Restoring Files to the Original Domain Controller

The following procedure restores the files to the original domain controller from the temporary domain controller. The temporary domain controller can be any additional server or backup domain controller if you have configured one. If you have a backup domain controller, the DCDB information should already have been copied from the original domain controller using the DCDB Replicator service. Make sure that all users are logged off before beginning.

This procedure does the following:

- Makes the original domain controller a server (with a role of Member) in addition to the temporary domain controller
- Restores the NET.ACC file on the original domain controller, which causes the user and group definitions to be copied to the originaldomain controller
- Restores default or backup 386 HPFS access control profiles on the original domain controller. (See the *Command Reference* for more information.)
- Copies the DCDB information from the temporary domain controller to the original domain controller

- Changes the temporary domain controller role to Member
- Changes the original domain controller role to Primary

To restore files to the domain controller:

1. Restore the NET.ACC file on the original domain controller by restoring the NET.ACC file to the proper directory.

   In addition to OS/2 Warp Server and its components (including User Profile Management), database manager and other program functions use the NET.ACC file. The NET.ACC file cannot be restored when these functions are active. For example, if any type of logon is issued before running a OS/2 Warp Server function, the NET.ACC file remains open and locked for the duration of the workstation session.

   In these cases, you must ensure that all autostart services are disabled before you can restore the NET.ACC file. To disable all autostart services:

   a. Copy and rename your STARTUP.CMD file (for example, STARTUP.BAK).

   b. Remove programs from the Startup folder.

   c. Comment out RUN statements in your CONFIG.SYS file that run OS/2 Warp Server, User Profile Management, or other programs that use the NET.ACC file.

   d. Close any running programs.

   After you have disabled the autostart services, restore the NET.ACC file as follows:

   e. If you have Local Security started, disable it by removing

      ```
      C:\IBMLAN\NETPROG\SECURESH.EXE
      ```

      from the PROTSHELL statement in the CONFIG.SYS file.

   f. Restart the system.

   g. Replace the NET.ACC file with the backup copy. At the command prompt on the original domain controller, type:

      ```
      COPY C:\IBMLAN\ACCOUNTS\NETACC.BKP C:\IBMLAN\ACCOUNTS\NET.ACC
      ```

   h. If you have 386 HPFS drives, use the RESTACC utility to restore the access control profiles that you previously backed up using the BACKACC utility. For example:

      ```
      RESTACC C:\ /S
      ```

      If you have multiple 386 HPFS drives to restore, issue the RESTACC command specifying the drive letter for each drive. See the *Command Reference* for more information.

   i. Reestablish your autostart services.

   j. Reestablish local security by changing the PROTSHELL= statement in the CONFIG.SYS file to:

      ```
      PROTSHELL=C:\IBMLAN\NETPROG\SECURESH.EXE C:\OS2\PMSHELL.EXE
      ```

   k. Restart your workstation and log on again as an administrator.

2. Change the role of the original domain controller to Member. At the command prompt, type:

   ```
   NET ACCOUNTS /ROLE:MEMBER
   ```

3. Start the original domain controller. At the command prompt, type:

   ```
   NET START SERVER
   ```

4. Copy the user and group accounts information on the temporary domain controller to the original domain controller. At the command prompt on the original domain controller, type:

   ```
   NET STOP NetLogon
   NET START NetLogon /UPDATE:Y
   ```

   These commands update the user and group accounts information to start within 60 seconds. Wait a few minutes for this copy process to be completed (depending upon the size of your domain and the number of users in the domain) before continuing to the following step.
5. Log on at the original domain controller with the user and administrator ID. For example, at the command prompt on the original domain controller, type:

   ```
   LOGON LANBKID /P:password
   ```

   If you do not plan to use the DCDB Replicator service to restore your DCDB, you can also log on through User Profile Management using the following command:

   ```
   NET USE Z: \\SRVRNAME\C$
   ```

   where Z: is the root drive of the additional server and C is the drive where OS/2 Warp Server resides.
6. After logging on, either use the DCDB Replicator service or issue the following commands to restore the files from the temporarydomain controller:

   ```
   XCOPY Z:\IBMLAN\DCDB C:\IMBLAN\DCDB /S /E
   ```
7. Log off. At the command prompt on the original domain controller, type:

   ```
   LOGOFF
   ```

   You can also log off through User Profile Management.
8. Change the role of the original domain controller to Primary. At the command prompt on the domain controller, type:

   ```
   NET STOP NetLogon
   NET ACCOUNTS /ROLE:PRIMARY
   ```
9. Change the role of the temporary domain controller to Member, or, if your temporary domain controller was a backup domain controller, to Backup. At the command prompt on the temporary domain controller, type:

   ```
   NET STOP NetLogon
   NET ACCOUNTS /ROLE:MEMBER
   ```

   Until the role is explicitly changed by another NET ACCOUNTS command, this server automatically starts up as an additional server.
10. Stop and restart the Server service on both the original and temporary domain controllers. At the command prompt on both workstations, type:

    ```
    NET STOP SERVER
    NET START SERVER
    ```
11. If the DCDB Replicator service is already started, replication does not occur. To begin replicating, you must first stop and then restart the service from an OS/2 command prompt by typing:

    ```
    NET STOP DCDBREPL
    NET START DCDBREPL
    ```

Users can log on to the domain and access resources (printers, files, applications, serial devices, and home directories) on the domain controller. Users who are logged on to the domain when you change the role of the servers must log off and log back on after the servers are restarted.

Allowing Adequate NET.ACC Synchronization Time

When additional servers or backup domain controllers are synchronized with the domain controller, no messages are displayed to indicate when synchronization has completed. Therefore, it is important to allow adequate NET.ACC synchronization time during certain procedures. Otherwise, you may encounter unexpected or undesired results.

For example, if you are using a REXX command file to set up the accounts and shared resources, you need to be aware of the propagation time. For example, if you define an alias for a resource on a remote workstation and then immediately try to define the access profile for that resource, the operation will fail with a message telling you `resource not found` because the NET.ACC which contains the definition for that alias has not been replicated to the additional servers yet.

Another situation where synchronization is important is during disaster recovery. For example, if you use a backup domain controller during primary domain controller failure, the time you allow for NET.ACC synchronization is critical to successful recovery. If the backup domain controller is promoted to a primary role because of a long downtime on the failed domain controller, the main NET.ACC file now resides on the temporary domain controller.

Eventually, when you switch the roles back (once the domain controller is repaired), the domain controller needs to come up as a member first in order to copy the NET.ACC. At this point, if you prematurely restore the original roles, the NET.ACC can end up in an incomplete state, and it would be very difficult to recover the lost information. Be sure to allow enough time for NET.ACC replication on the domain controller before changing servers back to their original roles.

Identifying Server Problems

Use the following procedure to identify a problem with your server. If the hard disk does not start the system, start it from OS/2 installation diskettes. Insert the *OS/2 Install Diskette* and then insert *Diskette 1* when prompted to do so. Press Esc from the first window, and make any necessary changes to the files on the hard disk. If you need more information, refer to the *Serviceability and Troubleshooting Guide*.

To identify where a problem is occurring on a server:

1. Make sure that the PATH, LIBPATH, and DPATH statements in the CONFIG.SYS file are intact.
2. Rename the STARTUP.CMD file. This action removes all automatic start actions. See Restoring files to the domain controller for more information about disabling the autostart features of OS/2 Warp Server.
3. Try to start the server.

   If the system starts, go to step 10 on page 30.

   If the system does not start, the problem is in the CONFIG.SYS file. Go to the following step.
4. Disable the NETWKSTA.200 line by adding REM at the start of the line:

   ```
   REM IFS=C:\IBMLAN\NETPROG\NETWKSTA.200 /I:C:\IBMLAN
   ```

   If you can start the system now, the NETWKSTA.200 line contains an error. This line reads the Networks and Requester sections of the IBMLAN.INI file. Go to the following step.

5. Check for an error on the NET1 line or for a workstation name that is not valid in the Requester section. Be sure that the X1, X2, and X3 values are adequate for your network. For more information on calculating these resources for your network, refer to *Quick Beginnings*. For more information about the IBMLAN.INI file and the NETWKSTA.200 line, refer to *Performance Tuning* .

   If the system still does not start, go to step 6.

6. Disable the following LAN drivers by adding REM at the start of the lines in the CONFIG.SYS file that include the LAN drivers:

   - ELNKII.OS2
   - ELNKMC.OS2
   - IBMNET.OS2
   - IBMNETA.OS2
   - IBMTOK.OS2
   - IBMTRBM.OS2
   - LANDD.OS2
   - MACWDAT.OS2
   - MACWDMC.OS2
   - NETBEUI.OS2
   - UBNEIPC.OS2
   - UBNEIPS.OS2
   - MACETH.OS2
   - IBMXLN.OS2

   If you can start the system now, the problem is either in the LAN hardware or in the PROTOCOL.INI file.

   If you cannot start the system, the problem lies in the OS/2 program, not in the server. Go to the following step.

7. Enable the NETWKSTA.200 line by removing REM at the start of the line:

   ```
   IFS=C:\IBMLAN\NETPROG\NETWKSTA.200 /I:C:\IBMLAN
   ```

8. Use the OS/2 installation diskette to copy the OS2.INI and OS2SYS.INI files from backup or from another workstation.

   If the LAN drivers and NETWKSTA.200 file initialize properly, go to the following step.

9. At the command prompt, type:

   ```
   NET START REQUESTER
   ```

   If the Requester service does not start, start other OS/2 Warp Server or LAN Server services in the IBMLAN.INI file by typing each of the following commands, one at a time:

   ```
   NET START REQUESTER /WRKS:
   NET START LSCLIENT
   NET START service
   ```

   where *service* is any other service in the **wrkservices** parameter of the IBMLAN.INI file.

   Make a note of any error messages that are displayed, and refer to the ERROR.TXT file for more information.

   If the Requester service starts, continue with step 10 on page 30.

10. At the command prompt, type:

    ```
    NET START SERVER
    ```

    If the Server service does not start, start other OS/2 Warp Server or LAN Server services in the IBMLAN.INI file by typing each of the following commands, one at a time:

    ```
    NET START SERVER /SRVS:
    NET START LSSERVER
    NET START service
    NET START NetLogon
    ```

    where *service* is any other service in the **srvservices** parameter of the IBMLAN.INI file.

    Make a note of any error messages that are displayed, and refer to the ERROR.TXT file for more information.

    If the `NET START NetLogon` command is unsuccessful, the problem is probably caused by the NET.ACC file. See Restoring files to the domain controller for instructions on restoring the NET.ACC file.

For more information, see the following topic:

- “Resynchronizing Passwords with the NetLogon Service”

Resynchronizing Passwords with the NetLogon Service

The server user IDs and passwords validate the identity of servers that receive copies of the NET.ACC file. Passwords can become unsynchronized when you use the NetLogon service if you:

- Reinstall a default or backup NET.ACC file onto an additional or backup server
- Reinstall a default or backup NET.ACC file onto the domain controller
- Inadvertently change an additional or backup server’s password on the domain controller without the new password being replicated to the additional or backup server before the next time NetLogon uses it
- Change passwords as a network error occurs during normal server operation
- Shut down an additional or backup server while the domain controller continues to run

This procedure describes how to resynchronize an additional server’s password with the domain controller. You work at the domain controller initially, and finish at the additional server (unless the additional server is a Windows NT server, in which case you work only at the domain controller). “Solutions to Resynchronization Problems” on page 32 provides steps for solving problems if the resynchronization fails.

To resynchronize passwords with the NetLogon service:

At the domain controller:

1. Open **LAN Server Administration**.
2. Open the appropriate domain object.
3. Open **Defined Servers**.

   Ensure that there is an object for the additional server.
4. If the additional server does not exist:

   a. Drag the **Server Template** to an open area in the Defined Servers folder.

      The Defined Server - Create notebook is displayed.
   b. Complete the Identity page.
   c. Select **Create**.
5. Open the appropriate server.
6. Open **Services**.
7. With mouse button 2, select **NetLogon Service**.
8. Select **Start**. The NetLogon service starts.

At the additional server:

1. Enter the following command at the OS/2 prompt:

   ```
   NET START SERVER
   ```

   The additional server attempts to start. If it fails to start, continue with the next step to resynchronize the additional server's internal password with the domain controller.
2. Enter the following command:

   ```
   LOGON USERID /P:PASSWORD
   ```

   This command uses the default user ID and password to log you on to the domain.
3. Enter the following command:

   ```
   NET STOP SERVER
   ```

   This command stops all server services.
4. Enter the following command:

   ```
   NET USER servername newpasswd
   ```

   where:

   servername Is the name of the failing additional server.

   newpasswd Is the new password for the additional server.

   This command sets the additional server's password on the domain controller.
5. Enter the following command:

   ```
   NET ACCOUNTS /ROLE:STANDALONE
   ```

   This command sets the additional server's role to stand-alone.
6. Enter the following command:

   ```
   NET USER servername newpasswd
   ```

   where:

   servername Is the same name you entered in step 4.

   newpasswd Is the same new password you entered in step 4.

   This command sets the additional server's password locally.
7. Enter one of the following commands, according to your need:

   ```
   NET ACCOUNTS /ROLE:MEMBER
   ```

   or

```
NET ACCOUNTS /ROLE:BACKUP
```

The command you enter resets the additional server's role to either member or backup.

8. Enter the following command:

   ```
   NET START SERVER
   ```

   The NetLogon service starts the additional server. The server's internal password is synchronized with the domain controller.

For more information, see "Solutions to Resynchronization Problems".

Solutions to Resynchronization Problems

This section provides two possible solutions if the resynchronization procedure fails to start the additional server:

- "Resynchronization Problems - Solution A"
- "Resynchronization Problems - Solution B" on page 33

Resynchronization Problems - Solution A: Complete the next procedure if any of these statements about your resynchronization attempt are true:

- The default user ID in step 2 on page 31 (at the additional server) does not exist.
- The default password in step 2 on page 31 (at the additional server) does not exist.
- A command in the resynchronization procedure produces an `Access Denied` message.

Perform the following steps at the OS/2 prompt on the additional server:

1. Enter the following command:

   ```
   LOGON userid /P:passwd
   ```

   where:

userid	Is a valid user ID on the domain controller.
passwd	Is a valid password on the domain controller.

   This command logs you on the domain controller with an existing administrator ID.

2. Enter the following command:

   ```
   NET USER newuseridnewpasswd /ACTIVE:YES /ADD /PRIVILEGE:USER
   ```

   where:

newuserid	Is a new user ID.
newpasswd	Is a new password.

   This command adds a new administrator ID on the domain controller.

3. Enter the following command:

   ```
   NET ACCOUNTS /ROLE:STANDALONE
   ```

   This command sets the additional server's role to stand-alone.

4. Enter the following command:

```
LOGON userid /P:passwd /L
```

where:

userid Is a valid user ID on the additional server.

passwd Is a valid password on the additional server.

This command logs you on the additional server with an existing ID.

5. Enter the following command:

   ```
   NET USER newuseridnewpasswd /ACTIVE:YES /ADD /PRIVILEGE:ADMIN
   ```

   where:

   newuserid Is the same new user ID you entered in step 2 on page 32 of this solution procedure.

   newpasswd Is the same new password you entered in step 2 on page 32of this solution procedure.

   This command adds a new administrator ID on the additional server.
6. Enter one of the following commands, according to your need:

   ```
   NET ACCOUNTS /ROLE:MEMBER
   ```

   or

   ```
   NET ACCOUNTS /ROLE:BACKUP
   ```

   The command you enter resets the additional server's role to either member or backup.
7. Using the new administrator ID you created in this solution procedure, repeat the second half of the procedure in "Resynchronizing Passwords with the NetLogon Service" on page 30, starting with **At the additional server**, step 1.

Resynchronization Problems - Solution B: Complete the next procedure if the NetLogon service fails to start for any reason. This solution removes the additional server from the Servers group, deletes the user ID, and adds the server again as a new member.

Perform the following steps at the OS/2 prompt on the additional server:

1. Enter the following command:

   ```
   NET STOP REQ
   ```

   This command stops all services.
2. Enter the following command:

   ```
   NET START REQ
   ```

   This command starts only the requester service.
3. Enter the following command:

   ```
   LOGON USERID /P:PASSWORD
   ```

   This command uses the default user ID and password to log you on to the domain.
4. Enter the following command:

   ```
   NET GROUP SERVERS servername /D
   ```

where *servername* is the name of the failing additional server.

This command removes the server from the group.

5. Enter the following command:

   ```
   NET USER servername /D
   ```

   where *servername* is the name of the failing additional server.

   This command deletes the additional server's machine ID.

6. Enter the following command:

   ```
   NET USER servernamepasswd /ADD
   ```

   where:

   servername Is either the original name or a new name for the additional server.

   passwd Is either the original password or a new password for the additional server.

   This command redefines the server.

7. Enter the following command:

   ```
   NET GROUP SERVERS servername /ADD
   ```

   where *servername* is the name of the additional server.

   This command adds the server to the group.

8. Enter the following command:

   ```
   NET START SERVER
   ```

   The NetLogon service starts the additional server. The server's internal password is synchronized with the domain controller.

   If the NetLogon service still does not start, repeat the second half of the procedure in “Resynchronizing Passwords with the NetLogon Service” on page 30, starting with **At the additional server**, step 1.

Chapter 3. Using the Logical Volume Manager

The Logical Volume Manager (LVM) allows you to create and manage volumes on the hard disks in your system. LVM components are initially installed and configured during the OS/2 Warp Server for e-business installation process. For a detailed discussion of LVM, including information about using it during installation, see *Quick Beginnings*.

LVM provides both physical and logical views of the system. The physical view shows how the hard disks are configured. The logical view displays the volumes currently configured on the system. You can switch between the two views by selecting **View** from the toolbar and choosing the view you want.

Physical View

The physical view of LVM allows you to create and manage partitions on the hard disks in your system. This view has two windows to show how the disks are partitioned and the volumes that are associated with them. This view displays the partitions present on each hard disk, allowing you to create and manage individual partitions. When you select a partition, the details of that partition or the volume associated with that partition are displayed in the lower window.

The physical view includes the following information:

Logical Volume
The name that has been assigned to the volume. A volume consists of one or more partitions. It is assigned a drive letter and is treated as if it were a single, contiguous partition. You can specify the name with the Create Volume option, and you can change the name with the Set/Change Name on Volume option.

Partition Name
The name that has been assigned to the partition. You can specify this name with the Create Partition option.

File System Indicates the type of file system on the volume. Any volumes that have not been formatted will not have a file type indicated.

Size Indicates the size, in megabytes (MB), of the volume.

Drive Linking Indicates if drives are linked together to create volumes.

Logical View

The logical view displays the volumes, their size, the unused portion size, and the volume name, and it indicates if the volume is linked. You can use this view to create, delete, and name volumes.

The logical view includes the following information:

Volume Name The name that has been assigned to the volume. A volume consists of one or more partitions. It is assigned a drive letter and is treated as if it were a single, contiguous partition. You can specify the name with the **Create Volume** option, and you can change the name with the **Set/Change Name of Volume** option.

Size Indicates the size, in megabytes (MB), of the volume.

% Used Indicates the amount of space used on a volume.

Unused (MB) Indicates the usable free space, in megabytes (MB).

File System Indicates the type of file system on the volume. Any volumes that have not been formatted will not have a file type indicated.

Drive Linking Indicates if drives are linked together to create volumes.

You can perform the following tasks with LVM:

- Create compatibility volumes (partitions), which can be seen by previous versions of OS/2 and other operating systems
- Create logical volumes that span physical disks
- Expand logical volumes (for JFS only)
- Delete compatibility volumes (partitions)
- Delete logical volumes

LVM can also be used after installation to perform additional configuration, if necessary.

Creating a Volume

Use **Create Volume** to create a volume. A volume consists of one or more disk partitions. Each volume is then assigned a drive letter. Currently, volumes have drive letters assigned to them, but partitions do not. You can create two types of volumes:

- Bootable Volume
- Nonbootable Volume

Creating a Bootable Volume

A bootable volume is a volume that can be used to boot an operating system. Only compatibility volumes are bootable.

To create a bootable volume:

1. Select **Volume** from the toolbar.
2. Select **Create Volume**.
3. Select **Create Bootable Volume**.
4. Select the partition or free space to create the volume from.
5. Type the new volume name in the space provided.
6. Choose the new drive letter associated with the volume and press OK. The new volume name and drive letter is now displayed.

Creating a Nonbootable Volume

A nonbootable volume is a volume that cannot be used to boot an operating system. It can be a compatibility volume or an LVM volume.

To create a nonbootable volume:

1. Select **Volume** from the toolbar.
2. Select **Create Volume**.
3. Select **Create Nonbootable Volume**.

4. Select **Create Compatibility Volume** if you want the volume to be accessed by other operating systems and previous versions of OS/2. Otherwise, select **Create LVM Volume** if you want the volume to span multiple disks, support Bad Block Relocation, or eventually be expanded.
5. Select the partition(s) or free space to create the volume from.
6. Type the new volume name in the space provided.
7. Choose the new drive letter and press OK. The new volume name and drive letter are now displayed.

Changes are effective when you save the changes and exit LVM. The system will then attempt to add the new volume without rebooting; however, if the Disk Device Manager has exhausted its resources, the system will need to reboot to make the changes effective.

Changing a Drive Letter Assigned to a Volume

Use **Change Drive Letter Assigned to a Volume** to change the drive letter associated with an existing volume. The new drive letter association will then remain unchanged until you change the drive letter again or delete the volume.

Note: Changing the drive letter assigned to a volume can have unforeseen effects. As a minimum, the drive letter currently assigned to the volume must not appear in any path, dpath, or libpath statements in your **CONFIG.SYS** file. Furthermore, the drive letter should not be referenced in any of the **.INI** files on the system. If these conditions are not met, your system may not boot properly, and some programs may not run correctly.

To change the drive letter assigned to a volume:

1. Select **Volume** from the toolbar.
2. Select **Change Drive Letter Assigned to a Volume**.
3. Select the volume that you want to modify.
4. Choose the new drive letter and press OK. The new drive letter is now displayed.

Note: You can also change the drive letter by selecting the volume and using the right mouse button.

When the changes are saved, the system will attempt to change the driver letter assignment without rebooting; however, if the file system cannot be unmounted, or if the Disk Device Manager has exhausted its resources, the system will need to reboot to make the changes effective.

Note: This choice can also be used to make the volume visible to OS/2 after you have hidden it using **Hide the Volume from OS/2**.

Expanding a Volume

Use **Expand the Volume** to expand an LVM volume.

Note: You must be using the Journaled File System (JFS) to be able to expand a volume. Currently, FAT and HPFS file systems cannot make use of extra space. For these file types, you must reformat the volume. JFS uses the **EXTENDFS** utility to allow it to use the extra space. See the *Command Reference* for more information.

To expand a volume:

1. Select **Volume** from the toolbar.
2. Select **Expand Volume**.
3. Select the volume you want to expand.

A window is displayed, allowing you to specify volume options.

4. Make your selections in the window and press OK to activate your choices.

Setting or Changing a Volume Name

Use **Set/Change the Volume Name** to set or change the name of a volume. The volume name on the Boot Manager Startup menu is also changed, if applicable. The names you assign to volumes remain unchanged through rebooting and hardware changes, and they always identify the same area on the disk. Volume names can be up to 20 characters long, can be entered in mixed case, and can contain spaces.

To set or change a volume name:

1. Select **Volume** from the toolbar.
2. Select **Set/Change Name** on Volume.
3. Select the volume you want to change.
4. Type the volume name in the space provided and press OK. The new volume name is now displayed.

Note: You can also set or change the volume name by selecting the volume and using the right mouse button.

Deleting a Volume

Use **Delete Volume** to delete volumes. All partition structures associated with the volume will be removed from the associated hard disk(s).

To delete a volume:

1. Select **Volume** from the toolbar.
2. Select **Delete Volume**.
3. Select the volume you want to delete.
4. Press OK to delete the volume.

Note: You can also delete the volume name by selecting the volume and using the right mouse button.

Hiding a Volume from OS/2

Use **Hide the Volume from OS/2** to make a volume invisible to OS/2.

To hide a volume from OS/2:

1. Select **Volume** from the toolbar.
2. Select **Hide the Volume from OS/2**.
3. Select the volume you want to hide.
4. Press OK to hide the volume.

Note: Use **Change Drive Letter Assigned to a Volume** to make the volume visible to OS/2 again.

Unhiding a Volume from OS/2

Use **Change Drive Letter Assigned to a Volume** to make a volume visible to OS/2.

To change the drive letter assigned to a volume:

1. Select **Volume** from the toolbar.
2. Select **Change Drive Letter Assigned to a Volume**.
3. Select the volume that you want to modify.
4. Choose the new drive letter and press OK. The new drive letter is now displayed.

Note: You can also change the drive letter by selecting the volume and using the right mouse button.

When the changes are saved, the system will attempt to change the driver letter assignment without rebooting; however, if the file system cannot be unmounted, or if the Disk Device Manager has exhausted its resources, the system will need to reboot to make the changes effective.

Creating a Partition

Use **Create Partition** to create a new partition. You can create partitions for other operating systems that do not recognize LVM volumes or linked volumes. You can also use this option to create a partition of a specific size and to allocate it from the beginning or end or free space.

Note: Partitions no longer have drive letters associated with them. You must create a volume to assign a drive letter.

To create a partition:

1. Select **Partition** from the toolbar.
2. Select **Create Partition**.
3. Select the disk to create the partition from.

A window is displayed, specifying free space and size for the partition.

4. Press OK to activate your choices.

Note: You can also create a partition by using the right mouse button to select the free space you want to create the partition from.

Deleting a Partition

Use **Delete Partition** to delete a partition. You cannot delete a partition that is part of a volume.

To delete a partition:

1. Select **Partition** from the toolbar.
2. Select **Delete Partition**.
3. Select the partition you want to delete.
A window is displayed, confirming your choices.
4. Press OK to activate your choices.

Note: You can also create a partition by using the right mouse button to select the partition you want to delete.

Committing Changes

Use **Commit Changes** to commit any changes you have made up to this point. A window will display to confirm that you want to commit the changes. Once you press OK, the changes cannot be undone.

To commit changes:

1. Select **Tools** from the toolbar.
2. Select **Commit Changes**.
3. Press OK to commit the changes.

Changes are effective when you save the changes and exit LVM. The system will then attempt to add the new volume without rebooting; however, if the Disk Device Manager has exhausted its resources, the system will need to reboot to make the changes effective.

Chapter 4. OS/2 Warp Server Personally Safe n Sound (PSnS)

OS/2 Warp Server Personally Safe n Sound (PSnS) is a powerful backup utility that lets you safe-guard your OS/2 system against loss of data. It allows you to set up a Backup Strategy for each activity you perform on your machine. The strategy, once employed, provides protection against all of the likely causes of data-loss: user errors, hardware malfunctions, malicious damage and disasters.

For more information about using PSnS, see the *OS/2 Warp Server Backup/Restore User's Guide* and the other online books that come with it. Also, additional information is available on the Internet at http://www.software.ibm.com/os/warp/warp-server.

Chapter 5. Managing Users and Groups

This chapter discusses how you can manage users and groups through LAN Server Administration. If you want to manage users and groups through User Profile Management as in previous versions of OS/2 Warp Server and LAN Server, refer to “Appendix B. User Profile Management” on page 261.

Notes:

1. If you are running other subsystems such as database manager or Communications Manager, you may need to use the User Profile Management interface to perform your user and group management functions. To accessUser Profile Management, open **UPM Services** located on your desktop.
2. In addition to the normal *domain logon* which is required for all users, LAN Server Administration provides a *local logon* facility for users who need to log on locally to their workstation. Users who have subsystems such as database manager may need to log on locally to access databases on their workstation. If you do not run subsystems requiring local logon, you can bypass the local logon option.

You can perform more user and group management functions with LAN Server Administration than with User Profile Management. Some of the functions available only from LAN Server Administration are:

- The capability to define up to 16,000 users per domain
- User and group ID cloning

  Cloning saves time by allowing you to use your mouse to take existing user and group objects and make clones (copies) that can be renamed and changed as required.
- Drag and drop enablement for logon assignments, user and group definitions

  You can drag and drop aliases onto user and group objects to create logon assignments automatically. In addition, you can drag and drop user accounts into groups, or groups into user accounts, to update a user or group definition automatically.
- The ability to define home directories for users

  You can specify home directories on a server for a user’s personal use.
- The ability to set directory limits on users

  You can set size limits on home directories. Alerts are sent to the users when the space used is nearing the limit.

You must define new users to the network so they can log on and access network resources. You can also define groups for access and messaging purposes. This chapter describes how to define and manage users and groups and how to create guest accounts.

The following tasks for managing users are discussed:

- Adding a user
- Cloning a user
- Deleting a user
- Updating user passwords and password requirements
- Granting and revoking operator privileges
- Updating user account information
- Updating user logon conditions

- Adding a user to a group
- Removing a user from a group
- Updating logon assignments
- Updating public applications on user's program starters
- Assigning a home directory
- Setting a user password expiration period for the domain
- Creating a logon profile

The following tasks for managing groups are discussed:

- Adding a group
- Cloning a group
- Viewing a group
- Updating a group
- Deleting a group
- Adding and removing users from groups

For more information, see the following topics:

- "Domain User and Group Definitions"
- "User ID and Group ID Management" on page 45
- "Managing Users" on page 47
- "Managing Groups" on page 58
- "Creating Guest Accounts" on page 61
- "Creating a Logon Profile" on page 62

Domain User and Group Definitions

OS/2 Warp Server and LAN Server allow the user and group definitions file (created and updated through LAN Server Administration or User Profile Management) to be centralized. This file is named NET.ACC and is maintained on the domain controller. Whenever a change is made to the user and group definitions, the changes are sent from the domain controller to all servers that are running the NetLogon service in the domain. The NetLogon service allows a server (except for Windows NT servers, which use a different version of the NetLogon service, IBMlogon) to receive changes to the user and group definitions file (NET.ACC).

When the user and group definitions file is updated, the NET.ACC file is not immediately replicated at the additional servers on the domain. The time it takes to update depends on when the update was made in relation to the value specified with the **pulse** parameter in the NetLogon section of the IBMLAN.INI file. This value indicates how often (in seconds) changes to the NET.ACC file are replicated to the additional servers. OS/2 Warp Server and LAN Server provide a feature called *forwarded authentication* that allows a defined user with a changed password to access resources on additional servers even if the NET.ACC changes have not reached the additional servers. Forwarded authentication is not available for new users.

You can log on to a domain and make changes to user and group definitions from any workstation on the network. The changes are made to the master copy at the domain controller, and changes are sent to all servers that are running the NetLogon service.

Note: LAN clients do not get copies of the NET.ACC file changes. Therefore, if user and group definitions are needed locally for an application (such as database manager), users must also be defined on the LAN Requester workstation through User Profile Management for the database manager requirements.

OS/2 Warp Server and LAN Server also allow users with Accounts operator privilege to manage users and groups. Accounts operators can create new users, modify user accounts, and manage group definitions. However, they cannot create or manage administrators or other operators. See “Granting and Revoking Operator Privileges” on page 50 for more information.

User ID and Group ID Management

LAN Server Administration provides the following processes to manage user and group IDs on the network. User Profile Management is used for user ID validation. Each installation of the User Profile Management is local to the particular workstation where it is installed, and it validates users who access controlled data or use programs that reside on that particular workstation.

Note: Local logons are used only when you have other subsystems (such as database manager) that require validation for access to local databases. If you are running only OS/2 Warp Server or LAN Server, you can bypass the local logon window.

For more information, see the following topics:

- “Password and ID Character Restrictions”
- “National Language Support Restrictions” on page 47

Password and ID Character Restrictions

OS/2 Warp Server and LAN Server can use either of two character sets:

expanded This character set can be used with High Performance File Systems (HPFS) and Journaling File System (JFS).

minimal This character set must be used with file allocation table (FAT) file systems and can be used with HPFS and JFS.

Note: National Language Support users should see “National Language Support Restrictions” on page 47.

The character set on HPFS and JFS can be changed by issuing the UPMCSET command: `UPMCSET /`*x*, where *x* is either `M` for minimal set or `E` for expanded set.

Rules for Both Character Sets

- Characters are converted to uppercase no matter how they are entered.
- User IDs and Group IDs cannot have the following values:

  - ADMINS
  - GROUPID
  - GUESTS
  - LOCAL
  - PUBLIC
  - RPLGROUP
  - SERVERS
  - SYSASID
  - USERS
- User IDs and Group IDs cannot begin with any of the following:
  - IBM
  - SQL
  - SYS

Rules for Expanded Character Set

- The number of characters (bytes) in each identifier can range as follows:

user ID	1 – 20
group ID	1 – 20
domain name	1 – 15
machine ID	1 – 15
password	0 – 14

  Notes:

  1. The actual minimum length for a password is set by the network administrator through the Policy page of the domain notebook. The network administrator also controls the number of passwords saved to prevent reuse, as well as the minimum amount of time that must pass before a user can change the password again.
  2. If a home directory is to be assigned to a user ID, the maximum length of the user ID can be 12 characters. The home directory is a shared network resource with the same name as the user account and cannot exceed 12 characters.
- The following characters can be used:
  - Upper or lowercase letters A to Z or any valid accented letter
  - Digits 0 to 9
  - Any special character that can be entered from the keyboard except for following characters:

    `" / \ [ ] ; : | < > + = , ? *`

Rules for Minimal Character Set

- The number of characters (bytes) in each identifier can range as follows:

user ID	1 – 8
group ID	1 – 8
domain name	1 – 8
machine ID	1 – 8
password	0 – 8

Note: By default, passwords are 4 to 8 characters in length.

- The following characters can be used:
  - Upper or lowercase letters A to Z
  - Digits 0 to 9
  - Special characters #, @ or $

Notes:

1. Other subsystems using the same user ID as OS/2 Warp Server and LAN Server may not necessarily have the same character limitations. Make sure your user ID does not violate the limitations of those subsystems.
2. The logon process may be unable to log on or access resources if the code page or country code of the system differs from those specified when the identifier was created. The user is responsible for ensuring the expanded character set is used only when the code page and country code of the system are not changed.

National Language Support Restrictions

National Language Support (NLS) users at DOS LAN Services cannot necessarily use all characters included in the User Profile Management expanded character set. Follow the DOS guidelines for acceptable accented characters, except for those in the following list.

COUNTRY or LANGUAGE	**PERMITTED CHARACTERS**
France (FR)	A — Z, 1 — 9, and nonalphabetics
Canadian French (CF)	A — Z, 1 — 9, and nonalphabetics
Portugal (PO)	A — Z, 1 — 9, Ñ, and nonalphabetics
Spain (SP)	A — Z, 1 — 9, Ñ, Ç, and nonalphabetics
Latin America (LA)	A — Z, 1 — 9, Ñ, and nonalphabetics
Japan	A — Z, 1 — 9, nonalphabetics, Kanji, Hiragana, and Katakana
Korea	A — Z, 1 — 9, nonalphabetics, Hanja, and Hangeul
Taiwan	A — Z, 1 — 9, nonalphabetics, and Hanzi

Managing Users

This section describes the basics of managing users: adding, cloning, deleting, and updating. If you are managing users in WorkSpace On-Demand 1.0 or 2.0 and want more information on these specific clients, please refer to the *WorkSpace On-Demand 2.0 Administrator's Guide*.

For the following procedures, you are making changes to the user and group definitions file (NET.ACC) for the one or more domains that you are managing.

Note: For Windows NT servers there are persistent users and localgroups, which are managed solely by the Windows NT server. To add or update these definitions, follow steps a through h of the directions for creating a Windows NT server definition. All other users and localgroups for the NT Server should be administered on the domain controller to prevent the NT server from being out of synch with the domain controller.

For more information, see the following topics:

- “Adding a User”
- “Cloning a User” on page 49
- “Deleting a User” on page 49
- “Granting and Revoking Operator Privileges” on page 50
- “Updating User Account Information” on page 51
- “Adding and Updating Logon Assignments” on page 53
- “Assigning Public Applications to Users” on page 55
- “Assigning a Home Directory” on page 56
- “Deleting a Home Directory” on page 57
- “Setting a User Password Expiration Period for a Domain” on page 58

Adding a User

You must add a user to the domain before that user can access the network. You can add approximately 16,000 users for each domain using LAN Server Administration.

Note: You can use the NET USER command to define about 1800 users on a domain. If you use User Profile Management to view user definitions, you can only see approximately 1260 users on each domain.

To add a user:

1. Open **LAN Server Administration**.
2. Open the appropriate domain object.
3. Open **User Accounts**.

   The User Accounts folder is displayed.
4. Drag a copy of the **Template** to a convenient location in the folder.

   The User Account - Create notebook is displayed.
5. Complete the required fields, indicated by an asterisk (*), and modify any other fields as needed.
6. Select the **Password** tab.

   The first Password page is displayed.
7. Select **Change password** to change the password.
8. Type the new password in the **New password** field.

   Note: For security purposes, the password is displayed as asterisks (*) when you type it.
9. Type the new password again in the **Confirmation** field.
10. Select the folded page corner to continue to the second Password page.
11. Complete the remaining fields on this page as desired.
12. Complete the fields on other pages as desired.
13. Select **Create**.

Cloning a User

Cloning allows you to save time when creating new users, by copying an existing user account object, renaming it, and modifying it as needed.

To clone a user:

1. Open **LAN Server Administration**.
2. Open the appropriate domain object.
3. Open **User Accounts**.

   The User Accounts folder is displayed.
4. With mouse button 2, select the user account you want to clone.
5. From the pop-up menu, select **Create another**.

   The User Account - Create notebook is displayed.
6. Type the new user account name in the **User account name** field.
7. Select the **Password** tab.

   The first Password page is displayed.
8. Select **Change password** to change the password.
9. Type the new password in the **New password** field.

   Note: For security purposes, the password is displayed as asterisks (*) when you type it.
10. Type the new password again in the **Confirmation** field.
11. Select the folded page corner to continue to the second Password page.
12. Complete the remaining fields on this page as desired.
13. Change any other fields at this time.
14. Select **Create** to create the new user ID. The new user ID inherits all the properties of the original user account.

Deleting a User

You can remove a user from the domain by deleting the user's user account. When you delete a user account, the following occurs:

- The user account is removed from the list of users.
- The user account is removed from all groups.
- The user loses access to network resources.

The directory path and the contents of the home directory for the user ID (if one exists) and its access control profile are not deleted. For more information on deleting the home directory, see “Deleting a Home Directory” on page 57. For more information on deleting the access control profile, see “Deleting an Access Control Profile” on page 96.

Attention: Do not delete system IDs for existing servers.

To delete a user:

1. Open **LAN Server Administration**.
2. Open the appropriate domain object.
3. Open **User Accounts**.

   The User Accounts folder is displayed.

4. Select the user account object you want to delete.
5. Press mouse button 2, and select **Delete**.
6. Select **Delete** on the confirmation window.

Granting and Revoking Operator Privileges

A user with operator privileges has certain administrative capabilities but is not a full administrator. A user may have one or more of the following types of operator privilege:

Accounts Can manage users and groups in the domain. The user can add, modify, or delete users and groups from either the command line or LAN Server Administration. The user cannot create or modify user accounts that have administrator or any operator privilege.

Print Can manage printer queues and print jobs. The user can create, modify, or delete printers or queues on servers in the domain, either from the command line or with LAN Server Administration. The user can also share printer queues and manage remote jobs on shared queues.

COMM Can manage serial devices. The user can share serial devices and manage remote jobs on shared serial devices from either the command line or LAN Server Administration.

Server Can manage aliases and other shared resources and view network status. The user can create, modify, or delete aliases or other shared resources from either the command line or LAN Server Administration.

A system administrator can use either the command line or LAN Server Administration to change operator privileges for users. See the *Command Reference* for more information about using the NET USER command to change operator privileges from the command line.

To change a user’s operator privileges:

1. Open **LAN Server Administration**.
2. Open the domain object.
3. Open **User Accounts**.

   The User Accounts folder is displayed.
4. Open the user account for which you want to change privileges.

   The first page of the notebook is displayed.
5. Select the **Privileges** tab.

   The Privilege page is displayed.
6. Select the **User** button.

   This choice denies administrator permissions to the user.
7. Select a **Special privileges** check box for each privilege you want to grant to the user.

   Deselect the check box to revoke the privilege.
8. Select **Set** or **Apply**.

Updating User Account Information

You can make updates to user account information through LAN Server Administration. The following information can be updated:

- User type (user, user with operator privilege, or administrator)
- Optional description about the user account
- Password
- Password options
- Home directory
- Logon workstation
- Logon authority (whether the user can log on to the domain)
- Group memberships (such as adding a user to a group and deleting a user from a group)
- Logon assignments
- Public applications

These tasks can be done through LAN Server Administration.

For more information, see the following topics:

- "Updating the User Account Description Field"
- "Updating a User's Password and Password Requirements"
- "Adding and Updating Group Memberships for a User" on page 52
- "Updating Logon Conditions for a User Account" on page 53

Updating the User Account Description Field

Use the following procedure to update user description fields.

To update a user account description:

1. Open **LAN Server Administration**.
2. Open the domain object.
3. Open **User Accounts**.

   The User Accounts folder is displayed.
4. Open the user account for which you want to update the user account description.

   The User Account notebook is displayed.
5. On the Identity page, update the description.
6. Select **Set** or **Apply**.

Updating a User's Password and Password Requirements

An administrator can change any password in the domain. Users can change only their own passwords.

Use the following procedure to reset a user's password and specify other password restrictions.

To reset or change a user password:

1. Open **LAN Server Administration**.

2. Open the domain object.
3. Open **User Accounts**.

   The User Accounts folder is displayed.
4. Open the user account for which you want to update the password.

   The User Account notebook is displayed.
5. Select the **Password** tab.

   The first Password page is displayed.
6. Select **Change password** to change the password.
7. Select **Expire password** if you want the user to change the password at next logon.
8. Type the new password in the **New password** field.

   Note: For security purposes, the password is displayed as asterisks (*) when you type it.
9. Type the new password again in the confirmation field.
10. Select the folded page corner to continue to the second Password page.
11. Complete the remaining fields on this page as desired.
12. Select **Set** or **Apply**.

See the NET USER command in the *Command Reference* for information on using the command-line interface to change password requirements.

Adding and Updating Group Memberships for a User

Once you have defined a user, you can add that user to one or more groups. You can also remove a user from a group.

To add or update group memberships for a user:

1. Open **LAN Server Administration**.
2. Open the domain object.
3. Open **User Accounts**.

   The User Accounts folder is displayed.
4. Open the user account for which you want to update the group memberships.

   The User Account notebook is displayed.
5. Select the **Groups** tab.

   The Groups page is displayed.
6. To add this user to a group:
   a. Select **Add** from the Groups page.

      The list of available groups is displayed in the Add User to Groups window.

   b. Select one or more groups to add this user to, and select **Add**.
7. To remove this user from a group, highlight one or more groups from the list and select **Remove**.
8. Select **Set** or **Apply**.

Note: You can perform the same task using drag and drop methods. You can drag and drop user accounts onto group objects or, alternatively, drag and drop group objects onto user accounts. When dropped, the group and user account definitions are automatically updated.

Updating Logon Conditions for a User Account

After you have defined a user, you can update logon conditions for the user account. You can set logon conditions such as:

- Deleting or disabling the user account
- Specifying whether the user account has an expiration date and time, and if so, what they are
- Specifying workstations that the user account can log on to.

To specify logon conditions for a user:

1. Open **LAN Server Administration**.
2. Open the domain object.
3. Open **User Accounts**.

   The User Accounts folder is displayed.
4. Open the user account for which you want to update logon conditions.

   The User Account notebook is displayed.
5. Select the **Account Info** tab.

   The first Account Info page is displayed.
6. Complete any required fields (indicated by an asterisk *) and any other fields as needed.
7. Select the folded page corner to continue to the second Account page.
8. Complete any remaining fields on this page as desired.
9. Select **Set** or **Apply**.

Adding and Updating Logon Assignments

You can define *logon assignments* for a user. Logon assignments give the user access to network resources by assigning resources to logical drives or ports each time a user logs on. The logon assignments remain in effect until changed. Both you and a user can change that user's logon assignments.

An alias must be defined for a resource before a resource can be defined as a logon assignment. See "Chapter 6. Sharing Network Resources" on page 65 for more information on defining aliases.

Before making logon assignments, you should create aliases for the shared resources you intend to define as logon assignments. You should also create an access control profile for that alias. See "Creating an Alias" on page 72 for more information.

You can add and update logon assignments either using the Assignments page of a user account notebook or using drag and drop methods. You can drag multiple users or groups onto alias objects in the appropriate Resource Definitions folder. The logon assignment to the alias is created when you drop the user or group onto the alias.

Alternatively, you can drag the alias object onto a user or group ID object. If you do not have an access control profile set up for the alias, you are prompted to create one during the drag and drop procedure. You can also remove logon assignments with the drag and drop method.

You can also update a user’s logon assignments from the command line with the NET USER command. For more information, see the *Command Reference* .

To add or update a user’s logon assignments:

1. Open **LAN Server Administration**.
2. Open the appropriate domain.
3. Open **User Accounts**.

   The User Accounts folder is displayed.
4. Open the user account object for which you want to update logon assignments.

   The User Account notebook is displayed.
5. Select the **Assignments** tab.

   The Assignments page is displayed.
6. If you want to change or remove a logon assignment, first select it from the list.
7. Select one of the following:
   - **Add** to add a new logon assignment
   - **Change** to change the selected logon assignment
   - **Remove** to remove the selected logon assignment

   The Logon Assignments window is displayed if you selected either **Add** or **Change**.
8. Complete the selections in this window, and select **OK**.
9. Select **Set** or **Apply**.

To add or update logon assignments with drag and drop:

1. Open **LAN Server Administration**.
2. Open the appropriate domain object.
3. Open one of the following objects that contains the user account or group for which you want to add or update logon assignments:
   - **User Accounts**
   - **Groups**
4. Open the appropriate Resource Definitions folder, which is also located in the domain container. For example, to add a directory as a logon assignment, open **Directory Resource Definitions**.

   All the available aliases in the domain are displayed.
5. Drag and drop the user account or group object onto the alias object to create or update a logon assignment.

   The Grant Access to a Resource window is displayed to allow you to grant access.

   Note: You can select multiple users or groups for drag and drop by pressing and holding the Ctrl key while selecting them. You can also drag alias objects onto user account or group objects.
6. If you want to add or change access permissions for the users, select the permissions you want to grant and indicate whether you are adding or replacing the permissions and then select **Set**.

   If you do not want to add or change permissions, select **Continue**.

   The Administer Logon Assignments window is displayed.
7. Complete the window to add, update, or remove the logon assignment.
   - To add or update a logon assignment:

a. Select **Add assignment**.
b. Select or type a drive letter or LPT or COM port for the logon assignment and then select other options as needed. The options are:
   - **Replace conflicting device assignments** to replace any resource already assigned to the specified drive or port.
   - **Replace existing logon assignments** to replace redundant assignments to the resource you selected.
c. Select **OK**.

   The Status window is displayed indicating the logon assignment has been added.
d. From the Status window, select **OK**.

- To remove a logon assignment:

a. Select **Remove assignment**.
b. Select **OK**.

   The Status window is displayed indicating the logon assignment has been removed.
c. From the Status window, select **OK**.

Assigning Public Applications to Users

You can make public applications available to users by assigning the applications to a program starter, which varies depending on the operating system.

For brevity, this chapter uses *program starter* as a general term to indicate where a user starts public applications. The program starter for OS/2 users is the Network Applications folder. The program starter for DOS users depends on whether they run Windows with DOS LAN Services (DLS).

For DLS machines with Windows, the program starter is the LAN Applications list, which is in the Application Installation window. For DLS machines without Windows, the program starter is the Run Applications window.

When a user logs on at a DOS client, the program starter includes any DOS applications, but no OS/2 applications, assigned to the user.

You can also remove public applications from a user’s program starter.

See “Chapter 9. Managing OS/2, DOS, WorkSpace On-Demand, and Windows Applications” on page 113 for information on defining applications.

Note: These instructions are for updating one or more user’s program starter while you are working with a specific user’s details. To add applications to or delete applications from several or all users’ program starters, see “Chapter 9. Managing OS/2, DOS, WorkSpace On-Demand, and Windows Applications” on page 113.

Adding applications to program starters makes it convenient for users to use their applications.

To add OS/2 or DOS applications to users’ program starters:

1. Open **LAN Server Administration**.
2. Open the appropriate domain object.

3. Open one of the following objects that contains the user account or group:
   - **User Accounts**
   - **Groups**
4. Open **Public Application Definitions**, which is also located in the domain collection.
5. Drag one or more user accounts or group objects to the public application object.

   The Add Public Application window is displayed to allow you to add this public application to the user or group when they log on. This window has no properties.
6. Select **OK**.
7. Select **OK** in the confirmation window.

Assigning a Home Directory

A *home directory* is an optional directory resource on a server assigned to one or more users. Only an administrator can assign a home directory to a user or change the drive assignment or path to a user's home directory.

When a home directory is assigned to or created for a user through LAN Server Administration, the user is connected to the home directory as a logon assignment. An access control profile granting all permissions to that user is automatically created. (The access control profile is not propagated to existing subdirectories.)

If you want other users to share the same home directory, you can either modify the access control profile or create home directories for other users, specifying the same drive and path.

You can perform this task through either LAN Server Administration or the command-line interface. If you use the command-line interface to create a home directory, neither the access control profile nor the home directory is automatically created. You must create the access control profile and the home directory separately. For information about creating home directories using the NET USER command, refer to the *Command Reference*.

To create a home directory or update the home directory's drive assignment:

1. Open **LAN Server Administration**.
2. Open the domain object.
3. Open **User Accounts**.

   The User Accounts folder is displayed.
4. Open the user account for which you want to assign or update the home directory.

   The User Account notebook is displayed.
5. Select the **Home Directory** tab.

   The Home Directory page is displayed.
6. Complete the fields in this page.

   Note: For users at DOS LAN Services workstations, you cannot specify Z as the drive assignment to the home directory. If a DOS LAN Services workstation requires remote IPL, you cannot specify Y or Z as drive assignments. These logical drives are reserved by OS/2 Warp Server and LAN Server.

7. Select **Set** or **Apply**.

Note: The CHKSTOR utility only provides information about how much space users are using from their home directories. It does not prevent them from exceeding the limit. If you want to enforce size limitations for users, you can use the command line or LAN Server Administration to set directory limits. For information on how to set limits on the size of directories and set up alerts that notify selected user IDs when various directories are nearing maximum capacity and when they are full, refer to “Chapter 8. Limiting Space within Directories on 386 HPFS Servers” on page 101.

Deleting a Home Directory

You can remove a user’s home directory assignment without deleting the directory itself. Only the assignment prevents the directory from being assigned to the user at logon. Use this procedure if the home directory or its subdirectories are still needed by other users. For example, if the directory is a home directory for several users, removing just the home directory assignment for one user does not affect home directory access for the remaining users.

Alternatively, you can remove both the user’s home directory assignment and the directory itself. The directory cannot be deleted through LAN Server Administration but can be deleted through the command line interface. Any files or subdirectories contained in the home directory are also deleted.

To remove a user’s home directory assignment without deleting the directory itself:

1. Open **LAN Server Administration**.
2. Open the domain object.
3. Open **User Accounts**.

   The User Accounts folder is displayed.
4. Select the user account for which you want to remove the home directory assignment.

   The User Account notebook is displayed.
5. Select the **Home Directory** tab.

   The Home Directory page is displayed.
6. Select **No home directory**.

   The link to the directory is broken, but the directory is not deleted.
7. Select **Set** or **Apply**.

For information on how to use the command-line interface to remove a user’s home directory assignment without deleting the directory itself, see the NET USER command in the *Command Reference*.

Setting a User Password Expiration Period for a Domain

OS/2 Warp Server and LAN Server allow you to set the duration for which user's passwords are valid. You can set this duration for all users who are defined in the domain by using LAN Server Administration.

To set a user's password expiration period:

1. Open **LAN Server Administration**.
2. With mouse button 2, select the domain object for which you want to set the password expiration period.
3. From the pop-up menu, select **Properties**.

   The notebook of the selected domain is displayed.
4. Select the **Policy** tab.

   The first Policy page is displayed.
5. Select **After** in the **Expires** section.

   Select or type the number of days you want the password to be valid.
6. Modify other fields on this page as needed.
7. Select **Set** or **Apply**.

You can also use the NET ACCOUNTS command and the **maxpwage** parameter to set an expiration period for a user's password. You can issue this command from an OS/2 command prompt while you are logged on at a client if you are using the NET ADMIN command or while you are logged on at a server.

The NET ACCOUNTS command can also be used to change the NetLogon service role, to specify how long a user can be logged on to the network beyond that user's normal logon hours, and to set the number of user passwords that must be unique through password changes. If the security features are being used, make sure that all administrator IDs are defined as requiring passwords.

For more information about the NET ACCOUNTS and NET ADMIN commands, refer to the *Command Reference*.

Managing Groups

OS/2 Warp Server or LAN Server can accept up to 256 group IDs per domain; however, nine group IDs are reserved for OS/2 Warp Server and LAN Server. Therefore, you can create up to 247 groups for your own use. The following IDs are reserved and should not be deleted:

- USERS (IDs with user privileges or groups of all user IDs)
- ADMINS (administrators)
- GROUPID (default group ID)
- SERVERS (servers defined in the domain)
- LOCAL (empty group used to grant permissions to the local workstation when no one is logged on)
- GUESTS (group or group of guest IDs)
- RPLGROUP (created only if Remote IPL is installed)
- SYSASID
- PUBLIC

Note: For Windows NT servers there are persistent users and localgroups, which are managed solely by the Window NT server. To add or update these definitions, follow steps a through h of the directions for defining a Windows NT Server. All other users and localgroups should be administered on the domain controller to prevent the NT server from being out of synch with the domain controller.

For more information about group ID restrictions, see “Password and ID Character Restrictions” on page 45.

For more information, see the following topics:

- “Adding a Group”
- “Cloning a Group”
- “Viewing a Group” on page 60
- “Updating a Group” on page 60
- “Deleting a Group” on page 61

Adding a Group

You can create user groups to refer to several users at the same time. On an OS/2 LAN, groups are used for access control and messaging purposes.

To add a group:

1. Open **LAN Server Administration**.
2. Open the domain object in which you want to add a group.
3. Open **Groups**.

   The Groups folder is displayed.
4. Drag a copy of the **Group Template** to a convenient position in the folder.

   The Group - Create notebook is displayed.
5. Complete the pages under each tab to add a group.
6. After you complete and check the properties, select **Create**.

Cloning a Group

If you want to set up a new group ID with characteristics similar to another group, you can clone the existing group ID, give it a new name and then make adjustments to it.

To clone a group:

1. Open **LAN Server Administration**.
2. Open the domain object in which you want to add a group.
3. Open **Groups**.

   The Groups folder is displayed.
4. With mouse button 2, select the group object you want to clone.
5. From the pop-up menu, select **Create another**.

   The Group - Create notebook is displayed.
6. Replace the name in the **Group name** field with the new group name.
7. If needed, select the **Users** tab to change the users in the newly created group.

8. Select **Create** to create the new group ID. The new group ID inherits all the properties of the original group.

Viewing a Group

You can view the list of users in a group after the group is created.

To view a group:

1. Open **LAN Server Administration**.
2. Open the domain object.
3. Open **Groups**.

   The Groups folder is displayed.
4. Open the group for which you want a list of users.

   The Group notebook is displayed.
5. Select the **Users** tab.

   The Users page is displayed, listing and describing all users in the group.

Updating a Group

You can add and remove users in a group after the group is created.

For more information, see:

- "Adding Users to a Group"
- "Removing Users from a Group" on page 61

Adding Users to a Group

Use the next procedure to add users to a group.

To add users:

1. Open **LAN Server Administration**.
2. Open the domain object.
3. Open **Groups**.

   The Groups folder is displayed.
4. Open the group you want to update.

   The Group notebook is displayed.
5. Select the **Users** tab.

   The Users page is displayed.
6. Select **Add**.

   The Add Users to Group window is displayed.
7. Select one or more users to add.
8. Select **Add**.

   The desired users are added.
9. Select **Set** or **Apply**.

Note: You can perform the same task using drag and drop methods. You can drag and drop user accounts onto group objects or alternatively, drag and drop group objects onto user accounts. When dropped, the group and user account definitions are automatically updated.

Removing Users from a Group

Use the next procedure to remove users from a group.

To remove users:

1. Open **LAN Server Administration**.
2. Open the domain object.
3. Open **Groups**.

   The Groups folder is displayed.
4. Open the group you want to update.

   The Group notebook is displayed.
5. Select the **Users** tab.

   The Users page is displayed.
6. Select one or more users to remove.
7. Select **Remove**.
8. When you finish removing users, close the notebook.
9. Select **Set** or **Apply**.

Deleting a Group

Besides removing users from groups, you can delete a group from the domain. Users in the deleted group no longer have permissions that may have been granted to them through membership in the group. However, deleting a group does not affect the individual user IDs and their associated user profiles.

Attention: Do not delete the groups named SERVERS, USERS, ADMINS, or any special group.

To delete a group:

1. Open **LAN Server Administration**.
2. Open the domain object.
3. Open **Groups**.

   The Groups folder is displayed.
4. With mouse button 2, select the group you want to delete.
5. From the pop-up menu, select **Delete**.
6. Select **Delete** in the confirmation window.

Creating Guest Accounts

If many users outside of your domain need access to one of your resources, you may want to create a *guest account*. A guest account for a resource gives any external user attempting to use the resource a specified access permission, without your having to define every user to the domain.

To set up a guest account, specify **guestacct=***userid* in the Server section of the domain controller's IBMLAN.INI file. The default is **guestacct=GUEST** (userid GUEST is used in the rest of the book). Refer to the *Command Reference* for more information on the NET USER command.

After the guest account is set up, any user not defined to the domain who attempts to use a resource in that domain (either through LAN Server Administration or with the NET USE command) is treated as the user GUEST. Multiple concurrent external users can access a domain resource using the guest account.

Resource access permissions given to user ID GUEST are given to users not defined on your domain. Any user ID can be identified as GUEST. When you set up access control permissions for resources, treat GUEST as any other user ID, but be aware that any user not specifically defined to the domain is given those same access permissions. All GUEST users receive the same access control profiles as the user specified on the **guestacct=***userid* line. For example, if the *userid* to which the GUEST ID is equated is that of an administrator, all GUEST users would have administrator privileges. For information on setting up access control profiles, see “Chapter 7. Defining Access Control Profiles” on page 83. For information on the IBMLAN.INI file, refer to *Performance Tuning*.

Notes:

1. Any user can log on to the domain using the guest ID defined in the IBMLAN.INI file. This logon does not prevent other users from accessing domain resources with the guest account permissions.
2. Do not delete the guest account and GUEST user ID from the remote IPL server. The guest account and GUEST user ID must be intact to allow the remote IPL workstation to gain access to the \IBMLAN\DCDB\IMAGES directory on the server. For more information on remote IPL, see “Chapter 16. Installing and Configuring Remote IPL” on page 207.
3. To enable DOS LAN Services users to change expired passwords at logon, you must either ensure that the server has a guest account or ensure that all DOS LAN Services client workstations have the OS/2 LAN APIs installed.

Creating a Logon Profile

You can create a *logon profile* for a user to gain access to certain files when logged on. A logon profile is a batch file containing commands that run automatically each time the user logs on. If you are using LAN Server Administration to create logon assignments for your users to access shared resources, you do not need to create logon profiles. However, some resources which are not shared by alias may be needed by a user at logon time. Use this procedure for those situations.

To create a logon profile for a user, create a file with one of the following required names:

- PROFILE.CMD for users at OS/2 clients
- PROFILE.BAT for users at DOS clients

The logon profile must be in that user’s user profile subdirectory,\IBMLAN\DCDB\USERS\ *userid*, for users at both OS/2 and DOS clients. If the subdirectory does not exist, create an alias for it. See “Appendix A. Directory Structure” on page 257 for more information on directory contents.

For example, for a user logging on to a DOS LAN Services client, the following line in the PROFILE.BAT file assigns printer alias LPT1Q to local printer LPT1:

```
NET USE LPT1: \LPT1Q
```

This command causes the DOS LAN Services workstation to connect to the printer resource at logon.

Notes:

1. User logon profiles can only be used with user IDs that do not exceed 10 characters. This restriction also applies when adding or changing logon profiles.
2. If your network has several servers acting as backup domain controllers, make sure user logon profiles are correctly stored on each of the backup domain controllers under the correct paths. Otherwise, if there is a domain controller failure, users will not be able to access their logon profiles from the backup domain controller.
3. Currently existing environment variables cannot be permanently set through the PROFILE.CMD or PROFILE.BAT file.
4. If you log on through UPM and your PROFILE.CMD file contains an ECHO or a SAY command, you receive a NET8195 error. To avoid this error condition, log on using the command-line interface.
5. If the PROFILE.CMD file is written in REXX language, you must have the `EXIT (0)` statement at the end of the file. Otherwise, a NET8195 error occurs.

You can also call other .CMD and.BAT files from a .CMD file or.BAT file associated with a user. This is a good way of creating a logon script that all users can run at logon time.

Chapter 6. Sharing Network Resources

Shared resources are directories, printers, and serial devices available to users of OS/2 Warp Server and LAN Server. Before users can assign a resource to a local device name, you must make the resource available by *sharing* it. After a user has redirected a device to the shared resource, requests to access the resource are granted only as specified in an access control profile.

Note:

> Clients can also share resources through the Peer service by using the NET SESSION, NET SHARE, NET START, and NET STATISTICS commands. For information about commands, see the *Command Reference*.
>
> Clients running OS/2 Warp with File and Print Client can share resources through the Shared Resources and Network Connections notebook.

For more information, see the following topics:

- “Types of Shared Resources”
- “How Resources Are Shared” on page 67
- “Using an Alias to Share a Resource” on page 70
- “Using a Netname to Share a Resource” on page 76
- “Connecting to Shared Resources” on page 79
- “Accessing Resources on Another Domain” on page 80
- “Examples” on page 80

Types of Shared Resources

The following types of resources can be shared:

- “Directory Resources”
- “Spooler Queues (Printers)” on page 66
- “Serial Device Queues” on page 66
- “Drives” on page 67
- “Resources on Servers in Other Domains” on page 67

Directory Resources

A *directory resource* is a directory or subdirectory on a server containing programs or data files that can be made available to users. When you give a user access to a directory resource, that user does not necessarily have access to the subdirectories and files contained in that directory resource. For more information about access control, see “Chapter 7. Defining Access Control Profiles” on page 83.

Spooler Queues (Printers)

You can determine which printers are shared, set up spooler queues, and decide whether to create printer pools. Printer port numbers range from LPT1 to LPT9. Printers are managed through individual printer objects.

A *spooler queue* is an ordered list of print jobs waiting to access a printer. For example, a spooler queue can contain jobs from several users to print on a specific printer. The jobs in a spooler queue are automatically routed to the printer. You can add, delete, and redefine spooler queues, as well as control print jobs and the printer status.

To make network printers available to users, you share spooler queues. As with other network resources, you can create aliases to identify spooler queues.

You can create printer pools for the network. A *printer pool* is a group of printers servicing a single spooler queue. Jobs on the spooler queue are printed on the first available printer in the pool.

Serial Device Queues

OS/2 Warp Server and LAN Server let you share serial devices, such as plotters, with users at OS/2 clients. Users at DOS clients can access serial printers set up as printer resources, but they cannot access other serial devices. You are responsible for defining serial device queues and pools and for authorizing users.

Notes:

1. Ensure that you have any COM.SYS device driver statements placed before the RDRHELP.SYS statement in the CONFIG.SYS file before defining an alias for a serial device queue. A COM.SYS device driver is added automatically when you choose to install serial devices during operating system installation. You can also copy the COM.SYS file from another server.
2. If more than two serial device queues or devices are created, the **maxchdevq** and **maxchdevs** parameters in the IBMLAN.INI file need to be increased. See *Performance Tuning* for more information about these parameters.
3. If handshaking is not specified for the serial device, device errors such as `Device offline` are not reported to the user. Handshaking for COM ports can be set anywhere a COM port icon is displayed.

1. Select the printer object on the desktop.
2. Select **Output**.
3. Select the COM icon of the printer's port.
4. Open the COM icon properties.
5. Set handshaking to either **Hardware** or **None**.
6. Select **OK**.

A *serial device queue* is an ordered list of network requests from users waiting to use a serial device. When the device becomes available, the client is connected to the device.

To make network serial devices available to users, you share serial device queues. As with other network resources, you can create aliases to identify serial device queues.

You can create *serial device pools* so that a request in the queue is sent to the next available device. You can assign priority levels to several queues connected to the same device or pool. In this way, a request in a high-priority queue to a device is processed before a request in a lower-priority queue.

Serial ports handle direct input/output. When you use a serial device queue, the *request* to use the device, rather than a file, goes into the queue. When a serial device becomes free, the request is granted and the direct input/output begins. The device is assigned to the requesting user.

While the serial device request waits in the queue, the user cannot continue with the present task. However, the user can do other OS/2 tasks. The amount of time the request remains in the queue is determined by the **charwait** parameter in the client's IBMLAN.INI file. For more information about the **charwait** parameter, refer to *Performance Tuning* .

Drives

A *drive resource* is a logical drive that contains a root directory and subdirectories that contain data files or application programs. Sharing a drive resource allows LAN users to connect to all data and applications on that drive.

Resources on Servers in Other Domains

In LAN Server releases before LAN Server Version 4, an *external resource* was a resource (directory resource, spooler queue, or serial device queue) on a server in another domain. Special configuration requirements and considerations were required. However, in OS/2 Warp Server and LAN Server, access to resources on servers in other domains is automatic. For this reason, such resources are no longer called external resources. If you have upgraded from a previous version of LAN Server, the external resources you defined are still available in OS/2 Warp Server.

In OS/2 Warp Server and LAN Server aliases used to represent resources on other servers are called *cross-domain aliases*.

How Resources Are Shared

You can share a resource by creating either a *netname* or an *alias* referring to the resource. A netname is a name that, in conjunction with the server name, identifies a resource on the network when the resource is shared. An alias is a resource definition that an administrator sets up for a directory, printer, or serial device on a particular server. All shared resources are assigned a netname, even if they are shared by the alias definition.

Aliases are the intradomain directory service for OS/2 Warp Server and LAN Server that makes connections to resources on multiple servers as easy as if there were one large server.

However, to manage who can access the shared resource, you should create an access control profile, as discussed in "Chapter 7. Defining Access Control Profiles" on page 83.

The netname of a resource on a server must differ from netnames of other resources on that server. However, the same netname can be used at other servers in the domain (possibly identifying a different resource at each server). Consequently, when referring to a resource by netname, the user must also specify the server where the resource resides. This combination of server name and netname is called the *universal naming convention (UNC)* name. The format for a UNC name is: `\\servername\netname\path`.

In contrast, resources with aliases can be referred to without specifying a server because the host server name is stored with the alias definition.

Another advantage of aliases is that they are more durable than netnames. Netnames are temporary because they are closely related to resource sharing. Resource sharing begins when a netname is created to refer to the resource. When sharing stops (perhaps because a server is stopped), the netname is discarded.

In contrast, an alias for a resource exists until you delete it. An alias definition contains information to create a netname and initiate resource sharing. This information enables OS/2 Warp Server or LAN Server to share the aliased resource automatically at server startup or at a user request. Or, if an aliased resource should not be shared automatically, it can be designated for sharing by administrator action only.

When a directory resource or serial device queue is shared by an alias, OS/2 Warp Server or LAN Server creates a netname, identical to the alias, at the server where the resource resides. For a printer queue, the netname matches the queue name rather than the alias. Thus, once shared, an aliased resource can be referred to both by its netname (and server) or by its alias.

If an alias is deleted while its resource is shared, sharing continues and the resource can still be referred to by its netname. You can stop this continued sharing, if desired, either before or after deleting the alias.

With the NET USE command, you can use the following $ shares. These items are shared automatically.

$ Share	**Description**
IPC$	The share for interprocess communication (IPC). Examples are named-pipe transactions.
ADMIN$	The share for remote command-line administration.
IBMLAN$	The share for all client access to the IBMLAN tree (mostly from the OS/2 Warp Server Administration).
D$	Every logical local drive on a server. For example, a server with drives C, D, and E has the following automatic $ shares made at server service startup: C$, D$, and E$.

Note: All $ shares are performed by the Server service except the IBMLAN share, which is performed by the LSServer service.

For more information, see the following topics:

- “Permitting Access to Shared Resources” on page 69
- “Specifying Maximum Concurrent Connections” on page 69

Permitting Access to Shared Resources

After you create an alias or a netname for a shared resource, create an access control profile to designate access permissions (such as read access) to the resource. A user may be able to access a file that has no access control profile if a profile exists for a drive or directory that contains that file and provides the user with the permissions to perform the requested action.

Note: Default access control profiles created by the network allow access to all spooler queues and serial devices. You can change these defaults by modifying the \PRINT and\COMM root profiles.

You can set up an access control profile in one of the following ways:

- The administrator is automatically prompted to create an access control profile when creating an alias.
- For an existing alias, you can select **Manage access** from an alias pop-up menu to access the window and create an access control profile for that resource (see "Creating an Alias" on page 72).

  Note: Only an administrator can create an access control profile. The administrator should give the P permission to operators or users so that they can manage access to this resource.
- From a current share on a server object, select the **Manage access** pushbutton on the Current Shares window.
- From the OS/2 Desktop, which is a local server:
  - You can select **Manage access** from the object pop-up menu of a local drive, directory, or file on your Desktop.
  - You can select **Manage access** from remote shared drive or directory in the IBM Network Resources folder.
- Through the NET ACCESS command. For more information, refer to the *Command Reference*.

Note: Only an administrator can create an access control profile. The administrator should give the P permission to operators or users so that they can manage access to this resource. Only an administrator or an operator or user with P permission can modify an access control profile.

For more information on access control, see "Chapter 7. Defining Access Control Profiles" on page 83.

Specifying Maximum Concurrent Connections

When you create an alias or share a resource by netname, the OS/2 Warp Server Administration displays an optional field called **Maximum concurrent connections**, which allows you to control how many users can use the resource at the same time (concurrent users).

For example, if you purchase 10 licenses to an application, you can install that application on a server, create a directory alias pointing to the subdirectory where the application resides, and specify **Maximum concurrent connections** as 10. The eleventh user trying to connect concurrently to the application cannot access it until one of the first 10 users releases the application. If you select **Unlimited**, an unlimited number of users can connect to the alias.

Using an Alias to Share a Resource

You can define aliases using LAN Server Administration, as discussed here, or by using the NET ALIAS command. For information about defining aliases with NET ALIAS, see the *Command Reference*.

Before users can access shared resources, access permission must be granted in an access control profile. For more information on access control, see "Chapter 7. Defining Access Control Profiles" on page 83.

You can make logon assignments either through aliases or with profile command files. Network application definitions can be created only with aliased directory resources. Resource connections established at the time network applications start must be aliased. Resources in multiple-server domains are easier to find if they are aliased.

In most cases users prefer to be connected to resources automatically at logon. The best way to do this in OS/2 Warp Server or LAN Server is to create an alias and make it a logon assignment for the users.

For more information, see the following topics:

- "Resources Requiring Aliases"
- "Alias Example"
- "Defining How and When Aliased Resources Are Shared"
- "Procedures for Using Aliases" on page 71

Resources Requiring Aliases

The following resources must be assigned using aliases:

- Resources that are logon assignments (directories, printers, or serial devices) for your users
- Network resources for shared public applications

Alias Example

Suppose directory EMP on SERVER1 contains employee data to be shared with network users. You could create an alias named EMPLOYEE for C:\EMP on SERVER1 and a short description, such as `Employee information`. The description is an optional field you can complete when creating the alias. Users see the alias and its description in the Identity page of the Alias notebook. In this example, the users see the following:

- `EMPLOYEE` is displayed in the **Alias** field.
- `Employee information` is displayed in the **Description** field.

Defining How and When Aliased Resources Are Shared

When defining an alias, you can choose to share the resource in different ways:

At server startup
This selection causes the resource to be shared immediately when the server on which it is located starts. It continues to be shared until the server is stopped, or until you explicitly stop sharing it.

Consider sharing frequently used resources, such as often-used printers and serial devices, at server startup. Also consider sharing at server startup those resources accessed from another domain.

When requested (for directory resources only)

This selection causes the resource to be shared dynamically when a user (with the appropriate access permission) requests to use that resource. A user can request use of a resource by:

- Logging on, thus invoking logon assignments
- Selecting a public application that uses network resources from the Network Applications folder
- Going through the Directory Resource Definitions folder and assigning the alias to a directory resource to start sharing

By administrator action

This selection causes a resource to be shared only when the administrator starts the sharing with LAN Server Administration or with the NET USE command.

When a resource is shared by administrator action, the sharing remains in effect until the server where the resource resides is stopped, or when you stop sharing the resource. The next time the server starts and a user needs to access that resource, you must share the resource again.

You can specify resource sharing by administrator action for resources over which you want more control. To access such resources, users must first contact you.

An attempt by a user from another domain to use a resource shared as required does not cause the resource to be shared.

When no user is using the resource, sharing is automatically stopped on when-requested aliases if the **cleanup** parameter is set to `YES` in the IBMLAN.INI file. If you have difficulty with drive disconnection, try adding `CLEANUP=NO`. Cleanup also affects nonaliased home directories.

Procedures for Using Aliases

When resources are shared, the issue of how the users access and share them must be addressed by the administrator. Most of this control is exercised through the assignment of aliases to the resources. Following are procedures for managing shared resources.

For more information, see the following topics:

- “Creating an Alias” on page 72
- “Updating an Alias” on page 73
- “Deleting an Alias” on page 73
- “Determining the Server on Which a Resource Resides” on page 74
- “Sharing Resources by Alias” on page 74
- “Viewing and Changing Share Details by Alias” on page 75
- “Giving Access to User Accounts and Groups” on page 75
- “Adding Resources for a Public Application” on page 75

- “Adding Public Applications for a User” on page 76

Creating an Alias

Creating an alias for a resource does not necessarily grant a user access to that resource. An administrator must also give each user the appropriate permissions. See “Chapter 7. Defining Access Control Profiles” on page 83 for information on access control profiles.

To create an alias for a resource:

1. Open **LAN Server Administration**.
2. Open the domain object in which you want to create the alias.
3. Open the appropriate Resource Definitions folder.
4. Drag the template for the type of alias object you want to create to a convenient location in the folder.

   The templates are **Printer Template**, **Directory Template**, and **Serial Device Template**.

   The appropriate alias notebook is displayed.
5. Type an alias name in the **Alias** field.
6. Optional: type a description in the **Description** field.
7. Select or type a server name:
   a. If the server where the resource is located is in this domain, select one of the server names in the **Server name** list.
   b. If the server where the resource is located is in another domain, type the name of that server in the **Server name** field.
8. Complete the other fields on the Identity page.

   Note: If you create more than two serial device aliases, you should increase the values of the **maxchdevq** and **maxchdevs** parameters in the IBMLAN.INI file.
9. Select **Create**.

   Note: If you are creating a directory alias and you specified a drive letter followed by a colon and a backslash (for example, F:\), a window is displayed requiring you to specify whether the access control profile is for the entire drive or for the root directory on the drive. This is an important consideration for removable media such as a CD-ROM, which should have the access control profile specified on the drive. Select **On drive** or **On directory**, and then select **OK**.

   - If there is no access control profile, a message is displayed prompting you to create one. Select **OK** to create the access profile.

     The Access Control Profile notebook is displayed.
   - If there is an access profile, no message appears. The Access Control Profile notebook is displayed.

   See “Chapter 7. Defining Access Control Profiles” on page 83 for information about access control profiles.
10. Complete the pages in the Access Control Profile notebook.
11. Select **Create** or **Set** to close the notebook.

    If it is a directory alias, a message is displayed prompting you whether to propagate the access permissions to all subdirectories in the path. See

"Propagating Access Control Profiles to Subdirectories" on page 88 for information about propagating (applying) an access profile to subdirectories.

12. Select **OK** to propagate access to all the subdirectories in the path, giving users Read (R), Write (W), and Create (C) access to the entire program directory tree.

    The alias is created, the resource is shared, and the access control profile is created. An icon representing the alias is added to the Resource Definitions object in the domain.

Updating an Alias

Use the next procedure to change the properties for an alias.

To update an alias:

1. Open **LAN Server Administration**.
2. Open the domain object in which you want to update the alias.
3. Open the appropriate Resource Definitions folder.

   The Resource Definitions folder is displayed.
4. Open the appropriate alias object.
5. Should you want to change the server name:
   a. If the server where the resource is located is in this domain, select one of the server names in the **Server name** field.
   b. If the server where the resource is located is in another domain, type the name of that server in the **Server name** field.
6. Further update the Identity page as desired.

   Note: If you create more than two serial device aliases, you should increase the values of the **maxchdevq** and **maxchdevs** parameters in the IBMLAN.INI file.
7. Select **Manage Access**.

   The Access Control Profile notebook is displayed.

   Note: Only an administrator, a user with operator privileges, or a user with P permission can modify an access control profile.

   An access control profile can be inherited automatically if the directory resource is either created remotely or resides on an HPFS or JFS drive and if the 386 HPFS is installed on the server. Even if an access profile is inherited, you may still need to modify the permissions.
8. Complete the pages in the Access Control Profile notebook.
9. Select **Set** to close the Access Control Profile notebook.

   If this is a directory alias, a message is displayed prompting you whether to propagate the access permissions to all subdirectories in the path. See "Propagating Access Control Profiles to Subdirectories" on page 88 for information about propagating (applying) an access profile to subdirectories.
10. Select **OK**to propagate access to all the subdirectories in the path.
11. Select **Set** again to close the alias notebook.

Deleting an Alias

You can delete one or more aliases from the domain.

Note: If the alias to be deleted is also a logon assignment, delete the logon assignment. Otherwise, the next time the user logs on, that user receives an error message indicating one or more logon assignments failed. For instructions on deleting logon assignments, see “Adding and Updating Logon Assignments” on page 53.

If the alias is shared at the time of its deletion, the sharing and the associated netname continue to exist. If an alias is created for a new resource using the deleted alias name and if users are connected to the original resource, accesses to that alias are to the original resource. To stop the sharing of a resource either before or after deleting its alias, refer to “Stopping the Sharing by Netname” on page 78.

To delete an alias:

1. Open **LAN Server Administration**.
2. Open the domain object that contains the alias.
3. Open the appropriate Resource Definitions folder.
4. With mouse button 2, select the alias object you want to delete.
5. From the pop-up menu, select **Delete**.
6. Select **Delete** in the confirmation window.

Determining the Server on Which a Resource Resides

You may occasionally need to check which server a resource is on or review how the alias is defined. For example, this ability is useful when deleting resources on a server. You can change a server on a OS/2 Warp Server or LAN Server Version 4 domain but not on down-level domains.

To display the server where a resource (alias) is located:

1. Open **LAN Server Administration**.
2. Open the domain that contains the alias.
3. Open the appropriate Resource Definitions folder.
4. Open the alias object you want to display information about.

   The alias notebook is displayed.
5. When finished viewing, select **Cancel**.

Sharing Resources by Alias

Use the next procedure to either start or stop resource sharing.

To start or stop the sharing of a resource by alias:

1. Open **LAN Server Administration**.
2. Open the domain object that contains the alias.
3. Open the appropriate Resource Definitions folder.
4. With mouse button 2, select the appropriate alias object.
5. From the pop-up menu, select one of the following as appropriate:
   - **Start Sharing**
   - **Stop Sharing**

Viewing and Changing Share Details by Alias

You can view and temporarily change a resource's sharing details, selecting the resource either by alias or by server and netname. The fields that can be changed are **Description** and **Maximum concurrent connections**.

To view and change the share details for an alias:

1. Open **LAN Server Administration**.
2. Open the domain that contains the alias.
3. Open the appropriate Resource Definitions folder.
4. Open the alias object you want to update.

   The alias notebook is displayed.
5. View or change the **Description** (after the alias is shared again).
6. View or change **When shared** and **Maximum concurrent connections** (after the alias is shared again).
7. If you change either, select **Set** or **Apply**.

   Any changes made do not take effect until the next time the alias is shared.

Giving Access to User Accounts and Groups

You can drag and drop a user account or group onto an alias object to give it access or logon assignments to the resource represented by that alias.

To drag a user account or group into an alias:

1. Open **LAN Server Administration**.
2. Open the appropriate domain object.
3. Open one of the following objects that contains the user account or group you want to provide access to this alias resource:
   - **User Accounts**
   - **Groups**
4. Open the appropriate Resource Definitions folder, which is also located in the domain container.
5. Drag the user account or group object to the alias object that represents the resource for which you are providing access.

   The Grant Access to a Resource window is displayed to allow you to grant access.
6. Complete the window.
7. Select **Set**.

   The Administer Logon Assignments window is displayed.
8. Complete the fields in the window.
9. Select **OK**.

Note: You can drag multiple users or groups onto alias objects in the appropriate Resource Definitions folder. You can also drag the alias object onto a user or group ID object.

Adding Resources for a Public Application

You can drag and drop an alias onto a public application object to allow assignment of the resource represented by that alias to a device when the application is run.

To drag an alias to a public application object:

1. Open **LAN Server Administration**.
2. Open the appropriate domain object.
3. Open **Public Application Definitions**.
4. Open the appropriate Resource Definitions folder.
5. Drag the public applications object onto the alias object that represents the resource to which you are providing access.

   The Assign Resource window is displayed.
6. Complete the window.
7. Select **OK**.

Adding Public Applications for a User

You can drag and drop one or more user account or group objects onto a public application object. This procedure adds the public application to the user’s Network Applications folder for OS/2, or Shared Applications window for DOS clients, or LAN Applications list for DOS LAN Services Windows.

To drag a user account or group to a public application object:

1. Open **LAN Server Administration**.
2. Open the appropriate domain object.
3. Open **User Accounts** or **Groups**.
4. Open **Public Applications Definitions**.
5. Drag a copy of the user account or group object to the public application object.

   The Add Public Application window is displayed to allow you to add this public application for each user at logon. This window has no properties.
6. Select **OK**.

Using a Netname to Share a Resource

Using a *netname* is another way to share a resource.

Sharing a resource by netname causes the resource to be shared only while the server where the resource resides is running (the current server session) or until you stop sharing the resource. The next time the server starts and a user needs to access that resource, you must share the resource again by doing one of the following:

- Selecting the **Share another** push button on the Current Shares window of a server object
- Selecting **Start share** from the menu of a local drive or file on your desktop
- Issuing the NET SHARE command

You can specify resource sharing by administrator action for resources over which you want more control. To access such resources, users must first contact you.

For users to access shared resources, access permissions must be granted in an access control profile. For more information on access control profiles, see “Chapter 7. Defining Access Control Profiles” on page 83.

For more information, see the following topics:

- “Sharing a Resource by Netname” on page 77

- “Stopping the Sharing by Netname” on page 78
- “Viewing and Changing Share Details by Netname” on page 78

Sharing a Resource by Netname

To share a resource without an alias, you must specify the location of the resource and give the resource a netname. Such sharing remains in effect only until the server with the resource is stopped or until sharing is stopped by the administrator.

To share a resource by netname through the OS/2 Warp Server Administration:

1. Open **LAN Server Administration**.
2. Open the appropriate domain object.
3. Open **Defined Servers**.
4. With mouse button 2, select the appropriate server object.
5. From the pop-up menu, select the arrow to the right of **Open as**.
6. Select the arrow to the right of **Current shares**.
7. From the following list, select the type of resource you want to start or stop sharing:
   - **Printers**
   - **Serial devices**
   - **Directories**

   A Current Shares window is displayed. It includes a list of resources defined on the domain as network resources currently shared.
8. Select **Share Another**.

   The Shared Resource window is displayed:
9. Type a unique netname in the **Netname** field.
10. Complete the remaining fields.
11. Select **OK**.

    If you are sharing a serial device queue, the queue is created at this point if it does not exist. The resource is then shared.
12. If you want to create or revise an access control profile for this resource, select **Manage Access** at the Current Shares window.

    Note: Only an administrator can create an access control profile. The administrator should give the P permission to operators or users so that they can manage access to this resource. Only an administrator or an operator or user with P permission can modify an access control profile.

    Directory resources require an access control profile before users can use them.

    The Access Control Profile notebook is displayed.
13. Complete the pages in the Access Control Profile notebook.
14. Select **Create** or **Set**.
15. Select **Close** to close the Current Shares window.

Stopping the Sharing by Netname

You can stop the sharing of a resource by doing one of the following:

- Using LAN Server Administration Current Shares window.
- Using the **Stop sharing** menu selection on the drive, directory, or printer object.
- Using the **Stop sharing** menu selection on the object in the File and Print Client Resource Browser folder (\\ *servername*\ *netname*) of the resource
- Using the NET SHARE command

Users currently using that resource are disconnected from it when the sharing is stopped.

When you stop sharing a spooler queue, the queue is not deleted. Spooled files already in the queue print until they are completed. However, any new spool file still being written is forced closed and does not print.

To stop sharing a resource by netname:

1. Open **LAN Server Administration**.
2. Open the appropriate domain object.
3. Open **Defined Servers**.
4. With mouse button 2, select the server for which you want to stop sharing the resource.
5. From the pop-up menu, select the arrow to the right of **Open as**.
6. Select the arrow to the right of **Current shares**.
7. From the following list, select the type of resource you want to stop sharing:
   - **Printers**
   - **Serial devices**
   - **Directories**

   A Current Shares window is displayed. It includes a list of resources defined on the domain as network resources currently shared.
8. Select the resource from the list.
9. Select **Stop share**.
10. Select **Close**.

You can also stop the sharing with the NET SHARE command.

Viewing and Changing Share Details by Netname

You can view and temporarily change a resource’s sharing details, selecting the resource by server and netname. The fields that can be changed are **Description** and **Maximum concurrent connections**.

To view and change sharing details of a resource by netname:

1. Open **LAN Server Administration**.
2. Open the appropriate domain object.
3. Open **Defined Servers**.
4. With mouse button 2, select the appropriate server object.
5. From the pop-up menu, select the arrow to the right of **Open as**.
6. Select the arrow to the right of **Current shares**.

7. From the following list, select the type of resource you want to view or change:
   - **Printers**
   - **Serial devices**
   - **Directories**

   A Current Shares window is displayed. It includes a list of resources defined on the domain as network resources currently shared.
8. Select the resource from the list.
9. Select **Change share**.

   The Change Share window is displayed.
10. View or change the **Description**.
11. View or change **Maximum concurrent connections**, which is the maximum number of connections defined for this resource.
12. Select **OK**.
13. If you want to create or revise an access control profile for this resource, select **Manage Access** at the Current Shares window.

    Note: Only an administrator can create an access control profile. The administrator should give the P permission to operators or users so that they can manage access to this resource.

    Directory resources require an access control profile before users can use them.

    The Access Control Profile notebook is displayed.
14. Complete the pages in the Access Control Profile notebook.
15. Select **Create**.
16. Select **Close** to close the Current Shares window.

Connecting to Shared Resources

For users to access shared network resources, a *local device name* can be assigned to the resource. For a directory resource, the local device name is a drive letter. For a printer or serial device, the local device name is a port number. Each logged-on user may have available local drives D through Z, COM ports 1 through 9, and LPT ports 1 through 9.

Note: For a startup drive on a remote IPL client, the drive ID C: is replaced with the remote IPL startup drive.

To connect to shared resources:

1. Open **LAN Server Administration**.
2. Open **Local Workstation**.
3. Select **Object**.
4. Select the arrow to the right of **Open as**.
5. Select **Current assignments**.
6. Select **Add**.

   The Add a Current Assignment window is displayed.
7. Select the resource type.
8. Select or type an alias or UNC name.

9. Type or select the local device used for this assignment.
10. Select **OK**.
11. Select **Close** at the Current Assignments window.

You can also use the File and Print Client Resource Browser or the NET USE command to connect to a resource. For more information, refer to the *OS/2 File and Print Client Guide* and the *Command Reference*.

Accessing Resources on Another Domain

To access a resource on another domain, a user must:

- Have a user account defined on the other domain. If the user account exists on the external domain, the password should be identical to that on the logon domain.

  DBCS Note: The following sentence does not apply to DBCS systems.

  In order for a PC LAN Program user to access an OS/2 Warp Server or LAN Server resource, the user's machine ID should be defined as a user ID on the OS/2 Warp Server or LAN Server domain.
- The user ID should be given the requested access permission on the other domain.
- Modify the 40th digit position of the IBMLAN.INI file wrkheuristics (called othdomains) with an ascii editor. Up to four other domains can ″know you″, your user ID and passwords. Use the same password in all domains. For more information about othdomains, see *Performance Tuning* or the command NET START REQUESTER in the *Command Reference*.

If you updated your othdomains there are three changes visible:

1. Inside the File and Print Client Resource Browser, there are more server icons.
2. NET VIEW command shows more servers.
3. In LAN Server Administration there are more servers in the icon view.

Examples

The following examples for sharing a CD-ROM drive are provided here:

- “Example: Sharing a CD-ROM Drive”
- “Example: Sharing a Directory on a CD-ROM Using an Alias” on page 81

Example: Sharing a CD-ROM Drive

The following example illustrates the steps required to share a CD-ROM drive on the network. After completing this procedure, all CD-ROM directories installed on this drive are shared.

To share a CD-ROM drive by alias and create an access control profile for it:

1. Open **LAN Server Administration**.
2. Open the domain in which you want to share the CD-ROM directory.

   Domains are represented by castle icons. The domain name is displayed under each icon.

3. Open the appropriate Resource Definitions folder.
4. Drag the **Directory Template** to an open area on the folder. The Identity page is displayed.
5. Complete the fields on the Identity page as follows:
   - **Alias Name:** CDDRIVE
   - **Description:** Nickname identifying shared CD-ROM drive
   - **Server:** SERVER1
   - **Path:** D:\
   - **When Shared:** At Server Startup
   - **Maximum concurrent connections:** Unlimited
6. Select **Create**.
   - If there is no access control profile, a message is displayed prompting you to create one. Select **OK** to create the access profile.

     The Identity page of the Access Control Profile notebook is displayed.
   - If there is an access profile, no message appears. The Identity page of the Access Control Profile notebook is displayed.

   Note: Only an administrator can create an access control profile. The administrator should give the P permission to operators or users so that they can manage access to this resource.
7. Select the **Permissions** tab.
8. Select **Add** under the list on the left.

   The Add Access Control Entries window is displayed. Select the user IDs or group IDs you want to access the drive. Select the permissions you want to grant to the users and groups you selected.
9. Select **OK**.
10. Select **Create**.

    The access control profile for the drive is created.
11. Select **Cancel**.

Example: Sharing a Directory on a CD-ROM Using an Alias

The following example illustrates the steps required to share a directory on a single CD-ROM using an alias. In this case, you must propagate the access control profiles in order for users to access all of the subdirectories on the CD-ROM directory.

Note: The term *propagate* is synonymous with the term *apply* used in versions of LAN Server before LAN Server Version 4.0. Because CD-ROM is removable media, the alias applies only to the CD-ROM inserted at the time the alias is created.

To create an alias for a CD-ROM directory:

1. Open **LAN Server Administration**.
2. Open the domain in which you want to share the CD-ROM directory.

   Domains are represented by castle icons. The domain name is displayed under each icon.
3. Open the appropriate Resource Definitions folder.
4. Drag the **Directory Template** to an open area on the folder. The Identity page of the notebook is displayed.

5. Complete the fields on the Identity page as follows:
   - **Alias Name:** CDDIR
   - **Description:** Nickname identifying shared CD-ROM directory
   - **Server:** SERVER1
   - **Path:** D:\ *directory*

     where *directory* is the directory path.
   - **When Shared:** At Server Startup
   - **Maximum concurrent connections:** Unlimited
6. Select **Create**.

   Note: If you are creating a directory alias and you specified a drive letter followed by a colon and a backslash (for example, F:\), a window is displayed requiring you to specify whether the access control profile is for the entire drive or for the root directory on the drive. This is an important consideration for removable media such as a CD-ROM, which should have the access control profile specified on the drive. Select **On drive** or **On directory**, and then select **OK**.

   - If there is no access control profile, a message is displayed prompting you to create one. Select **OK** to create the access profile.

     The Access Control Profile notebook is displayed.
   - If there is an access profile, no message appears. The Access Control Profile notebook is displayed.

   See “Chapter 7. Defining Access Control Profiles” on page 83 for information about access control profiles.
7. Select the **Permissions** tab.
8. Select **Add** under the list box.

   The Add Access Control Entries window is displayed.
9. Select the user IDs or group IDs you want to access the CD-ROM directory. Select the permissions you want to grant the users and groups you selected.
10. Select **OK**.
11. Select **Create** or **Set**.

    A message is displayed prompting you to specify whether to propagate the access control profile permissions to all the subdirectories in the path. See “Propagating Access Control Profiles to Subdirectories” on page 88 for information on propagating (applying) an access control profile to subdirectories.
12. Select **OK** if you want your users to access all the subdirectories of the directory you have shared.

    Select **Cancel** to give users access to only the directory you have shared; users can only access files in the indicated directory of the CD-ROM. You can propagate access to the other subdirectories at a later time.

    The alias (CDDIR) is created, the CD-ROM directory is shared, and the access control profile is created. An icon representing the alias is added to the Resource Definitions object in the domain.

Chapter 7. Defining Access Control Profiles

This chapter describes access control for resources accessed remotely on the LAN. As the network administrator, you are responsible for network security. Access control allows you to manage user access to network resources. In order to use the security features of OS/2 Warp Server or LAN Server, it is strongly recommended that your ID (as administrator) be defined as requiring a password. Administrators are not subject to access control.

Note: There are differences between the behavior of the access control system used in the HPFS and JFS and that used in the 386 HPFS. These differences are noted throughout the chapter.

All resources accessed from the network must have a set of permission rules defined for them. You can permit use of a resource by assigning *access permissions* to particular users or groups. When you create an access control profile for a resource, you can optionally set up an audit log to record access attempts to that resource.

You can protect the following:

- Directories (including files and subdirectories if the path exists)
- Printer spooler queues
- Serial device queues
- Printers
- Drives
- Files
- *Named pipes*. Named pipes allow two programs to communicate with each other. They are treated as directory resources. Named pipes must be preceded by \PIPE\.

For more information, see the following topics:

- “Access Control Profiles”
- “How Access Permissions Are Processed” on page 86
- “Access Control Profile Example” on page 87
- “Propagating Access Control Profiles to Subdirectories” on page 88
- “Procedures for Managing Access Control Profiles” on page 90
- “Default Access Control Profiles on Servers” on page 97
- “CD-ROM Devices and Access Control Profiles” on page 100

Access Control Profiles

Each protected resource has an *access control profile*. When you protect a resource, you define the users and groups who have access to the resource and their permissions.

An access control profile for a resource is independent of the resource’s alias or netname. You can create an alias or netname for a resource, and then create an access control profile for it.

Additional aliases for the same resource share the same access control profile. Modifying an access control profile for one alias modifies it for all aliases for the same resource.

For more information, see the following topics:

- “Access Permissions”
- “Profile Contents” on page 85

Access Permissions

The following list defines the access permissions you can specify in an access control profile.

Permission **Meaning**

Delete (D) Permits deleting subdirectories and files.

Attributes (A)
Permits changing of OS/2 file attributes, such as A (archive), R (read only), and related file information, such as the time and date the file was updated. Also, some applications may require attributes permission to copy files.

None (N) Denies access to the resource.

Execute (X) Permits only running (not copying) of program or command files, such as .EXE or .COM files.

Note: Besides execute permission, read permission is required for users to run .BAT files, .CMD files, and DOS applications. Because applications request read permission when they open a file for execution, provide read access permission for applications of this type.

Read (R) Permits reading and running of files in a directory, and copying of files from a directory, but not writing to (modifying) them. Lets users view file names in a shared directory. Read used alone lets users view or run programs only.

Write (W) Permits writing to (modifying) a directory resource in a shared directory. Write used alone lets users modify files but not read, run, create, or delete them. In most cases, and always when editing files, use write with read permission.

Directory resources with write (W) permission also need attributes (A) permission if they are used in applications that change file attributes.

Create (C) Permits creating of subdirectories and files in a shared directory. Create used alone lets users create a file in a directory and modify the file during its creation. However, once a file is created and closed, the same user cannot modify it again.

To write to a serial device, users must have both C and W permissions for the serial device.

To create and send a print job to a printer, users must have C permission for the printer.

To create a named pipe on a server, users must have C permission for named pipes.

Permissions (P)
Permits changing of resource access permissions, giving a user limited administrator authority over the resource. However, a user cannot create an access control profile.

These access permissions can be used in different combinations. However, not all permissions can be used with all resource types, as shown in the following table. When you create or update an access control profile, OS/2 Warp Server or LAN Server accepts permissions applicable to that resource type.

Table 1. Access Permissions Applicable to Resource Types

Permission	Files	Printers	Serial Devices	Named Pipes
None (N)	X	X	X	X
Execute (X)	X			
Read (R)	X		X	X
Write (W)	X		X	X
Create (C)	X	X	X	X
Delete (D)	X			
Attributes (A)	X			
Permissions (P)	X	X	X	X

Profile Contents

An access control profile for a resource can contain the following information:

- Descriptions of individual users and their access permissions, including:
  - User ID or group ID
  - Access permissions

  Note: The user accounts system defines a default group named GROUPID. It can be used as any other group, or it can be deleted.
- Recording of access attempts in the audit log. The audit log flag controls whether audit log records are written for accesses to the resource. The flag can have the following values:

  None Do not write records.

  All Write records for all accesses to the resource.

  Failures Write records only for failed accesses.

  Successes Write records only for successful accesses.

  For more information, see “Auditing” on page 151.

Note: An access control profile is limited to 64 entries of users or groups of users. Therefore, users with similar access permission requirements should be put into groups.

How Access Permissions Are Processed

Administrators are automatically granted all permissions by OS/2 Warp Server or LAN Server and are not subject to access control processing. For all other users, OS/2 Warp Server or LAN Server denies access to a resource unless you specifically grant access for a user ID or its corresponding group IDs. When a user attempts to use a resource, OS/2 Warp Server or LAN Server searches for that user ID in the resource's access control profile, checking first the user access profile and then the group access profile. The following steps describe the search procedure:

1. The program first checks to see if the user ID is profiled in the user access profile and, if so, what permissions are given to that user.
   - If the user ID is profiled and the requested permissions are included, the user gains access.
   - If the user ID is profiled and the requested permissions are *not* included, access is denied. No further checking for access permissions is done. That is, the program does not go on to check the group access profile.
   - If the user ID is not profiled, the program checks the group access profile. See step 2.
2. The program checks to see if the user belongs to any of the groups profiled in the group access profile and, if so, what access permissions are given to those groups.
   - All users are members of the group USERS.
   - If the requested permissions are included in the sum of the group access profile permissions, the user gains access. For example, if a user belongs to a group with W and A permissions, and the group USERS has R, W, C, and P permissions, the sum of the group access profile permissions is R, W, A, C, and P.
   - If the requested permissions are *not* included in the sum of the group access profile permissions, access is denied.

See “Access Control Profile Example” on page 87 for an illustration of how this works.

For more information, see the following topics:

- “Access Control Profile Searching”
- “Denying Access to a Directory Resource” on page 87

Access Control Profile Searching

The search for an access control profile proceeds in the following order:

1. Resource the user is trying to access
2. Directory of that resource (only applies to files)
3. Root (default permission) for that disk partition or resource type

   Note:

   Specify the drive (C:) to give default permissions to all files in all subdirectories. Specify the directory (C:\) to give access only to files in the root subdirectory.

For spooler queues, the root is \PRINT. For serial device queues, the root is \COMM. For named pipes, the root is \PIPE.

Once the program finds an access control profile, permissions are processed as described in “How Access Permissions Are Processed” on page 86, and the user may or may not gain access. The search does not continue once a profile is found at any of these three places.

For example, suppose a user tries accessing directory resource C:\SUBDIR\FILE.ONE. If there is an access control profile for the resource (FILE.ONE), the search stops and permissions in that profile are used. If no profile is found, the program checks whether there is a profile for the current directory, C:\SUBDIR. If there is a profile for the current directory, it is used. If a profile is not found, the program goes on to the root, C:\. If there is a profile for C:\, those permissions are used. If there is no profile at any of these three levels, the user is denied access.

Note: Access control checking for named pipes is handled in the same way as directory resources. The resource is checked first, the directory is checked second, and the root is checked last.

Denying Access to a Directory Resource

Because of the search process described in “Access Control Profile Searching” on page 86, a user might be able to gain access to a resource even if no profile exists for that resource. OS/2 Warp Server or LAN Server searches for the existence of an access control profile for that resource, then it searches for the parent, and then it searches for the root. If a profile exists and the user is listed in the access control profile, or if the permissions for the USERS group value is any value but none (N), the user has the access permissions specified.

To make sure a user has no access to a directory resource, create an access control profile for the resource, and specify N permission for that user ID in the user access profile. Access control should be done by group to ensure that the user is not in a group that has access. Delete any occurrences of the user ID in the profile. You only have to specify N if the user is a member of a group that has access and if you cannot delete that user from the group. The USERS group should be used only for resources that are widely used.

Access Control Profile Example

Figure 1 on page 88 shows a directory structure and the access control permissions for resources in the directory. The highlighted directories and files are those protected by access control profiles. Permissions included in the access control profiles are shown to the right of the protected resource. User KIM belongs to the group ACCTGRP.

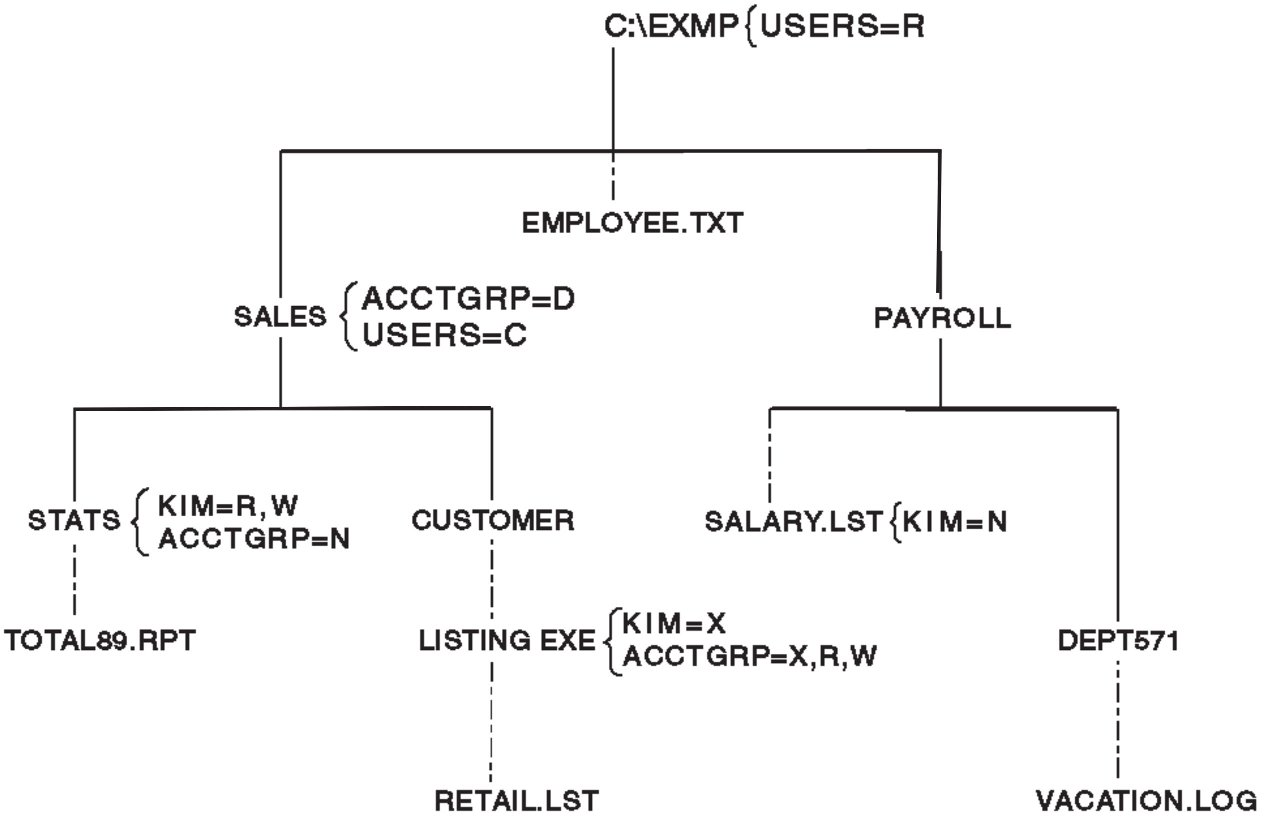


Figure 1. Access Control Profile Example

Given the directory structure and permissions in the previous figure:

- If user KIM tries to edit the file EMPLOYEE.TXT, an error occurs because the permission at the current directory C:\EXMP allows only read access.
- If user KIM tries to create or delete a file in the directory SALES, the operation succeeds because the combined group (ACCTGRP) permission and permissions for USERS group gives KIM create and delete permissions.
- If user KIM tries to edit the file TOTAL89.RPT, the operation succeeds because KIM has write and read permissions at the current directory, C:\EXMP\SALES\STATS. These permissions take precedence over none for ACCTGRP, because the program checks the user access profile first.
- If user KIM tries to copy the file LISTING.EXE, an error occurs because KIM has only execute permission. This permission takes precedence over execute, read, and write permissions for ACCTGRP.

Propagating Access Control Profiles to Subdirectories

The following discussion pertains only to directory resources.

After creating an access control profile for a directory resource, you can choose to *propagate* the profile to the subdirectories of that resource. When you *propagate* an access control profile for a directory, the permissions in that profile are used as a template propagating to all subdirectories beneath the directory. If an access control profile already exists for a subdirectory (or for any files in a subdirectory), it is overwritten with the permissions in the template profile. The existing profile's audit log setting is not modified by the propagate function. If an access control profile does not already exist for a subdirectory, a profile with the same permissions and audit log setting as the template profile is created. A profile is not created for a file that currently has no profile.

The propagate function makes sure all profiles in the directory and subdirectories contain only the permissions of the specified source profile.

Only administrators can propagate an access control profile.

You should not propagate access control profiles to the directory resource that contains the IBMLAN directory: \DCDB, \DOSLAN, \NETPROG, and \IBMLAN itself. Adhering to this rule prevents changes in the access control profiles of the subdirectories that could adversely affect your server. However, you can propagate access control profiles to users' home directories.

Remember the following about using the propagate function with the IBMLAN directory:

- You can propagate access control profiles to any subdirectories in the IBMLAN directory whose names begin with the letters RPL.
- If you propagate an access control profile to the root directory of the drive where the IBMLAN directory resides, OS/2 Warp Server or LAN Server skips the IBMLAN directory when altering access control profiles.

For more information, see the following topics:

- "Permissions Used when Propagate Is Not Used"
- "Propagate Example"

Permissions Used when Propagate Is Not Used

Propagating an access control profile is optional for administrators (users cannot propagate a profile). If you do not propagate an access control profile for a directory, it is used only for that directory and not copied to any subdirectories below the directory.

Propagate Example

Using the example shown in the previous figure, an access control profile is created for directory C:\EXMP with the following access permissions:

```
KIM=R,W
TESTGRP=R
USERS=N
```

The list below shows the example results of propagating the C:\EXMP access control profile.

Files Resource	**Result**
C:\EXMP	No change
C:\EXMP\SALES	Existing profile's permissions replaced
C:\EXMP\PAYROLL	Profile created

C:\EXMP\SALES\STATS
Existing profile’s permissions replaced

C:\EXMP\SALES\CUSTOMER
Profile created

C:\EXMP\SALES\CUSTOMER\LISTING.EXE
Existing profile’s permissions replaced

C:\EXMP\PAYROLL\DEPT571
Profile created

C:\EXMP\PAYROLL\SALARY.LST
Existing profile’s permissions replaced

C:\EXMP\SALES\CUSTOMER\RETAIL.LST
No change because no profile exists for this file

Procedures for Managing Access Control Profiles

This section contains procedures for managing access control profiles.

For more information, see the following topics:

- “Creating an Access Control Profile”
- “Updating an Access Control Profile” on page 93
- “Deleting an Access Control Profile” on page 96

Creating an Access Control Profile

There are two ways to create access control profiles:

- Through LAN Server Administration, for resources with and without aliases. This chapter describes the access control profile procedures performed with LAN Server Administration.
- At the OS/2 command prompt, using the NET ACCESS command. Refer to the *Command Reference*.

There are two other ways that access control profiles can be applied to a resource. These methods involve inheritance.

- Using a redirected drive remotely. When you create a directory while in a redirected drive, a new profile is created with the same permissions for the new directory.
- When you create a directory either locally or remotely on a 386 HPFS server, the newly created directory inherits the access control profile information of the parent directory. Because of the way the file allocation table (FAT) works, you can inherit only a remotely created directory’s access control profile on a FAT file server. You must have access to the access control profile on the server to be able to inherit it. You must be logged on with an ID that is allowed access to the parent access control profile. If successful, a new profile is created with the same permissions as the parent of the new directory.

  Inheritance is performed by the OS/2 Warp Server or LAN Server code. When a directory is created locally at a server using the standard OS/2 file systems (FAT, HPFS, and JFS), the OS/2 Warp Server or LAN Server code is not invoked and does not perform inheritance.

For information on what default access control profiles may already exist, especially on servers with local security, see “Default Access Control Profiles on Servers” on page 97.

The following tasks also include how to create an access profile for users and groups.

For more information, see the following topics:

- “Creating Access Control Profiles for Resources with Aliases”
- “Creating Access Control Profiles for Resources without Aliases” on page 92

Note: Only an administrator can create an access control profile. The administrator should give the P permission to operators or users so that they can manage access to this resource.

Creating Access Control Profiles for Resources with Aliases

When you create an alias for a resource, you are prompted about whether to create an access control profile as well. The following procedure is for creating both an alias and access control profile for the resource.

Note: Only one access control profile can exist for each resource, no matter how many aliases that resource has.

If you created an alias for a resource without creating an access control profile, use the procedure in “Updating Access Control Profiles for Resources with Aliases” on page 94 to create the access control profile.

Creating an alias for a resource does not necessarily grant a user access to that resource. An administrator must also give each user the appropriate permissions.

To create an alias for a resource:

1. Open **LAN Server Administration**.
2. Open the domain object in which you want to create the alias.
3. Open the appropriate Resource Definitions folder.
4. Drag the template for the type of alias object you want to create to a convenient location in the folder.

   The templates are **Printer Template**, **Directory Template**, and **Serial Device Template**.

   The appropriate alias notebook is displayed.
5. Type an alias name in the **Alias** field.
6. Optional: type a description in the **Description** field.
7. Select or type a server name:
   a. If the server where the resource is located is in this domain, select one of the server names in the **Server name** list.
   b. If the server where the resource is located is in another domain, type the name of that server in the **Server name** field.
8. Complete the other fields on the Identity page.

   Note: If you create more than two serial device aliases, you should increase the values of the **maxchdevq** and **maxchdevs** parameters in the IBMLAN.INI file.

9. Select **Create**.

   Note: If you are creating a directory alias and you specified a drive letter followed by a colon and a backslash (for example, F:\), a window is displayed requiring you to specify whether the access control profile is for the entire drive or for the root directory on the drive. This is an important consideration for removable media such as a CD-ROM, which should have the access control profile specified on the drive. Select **On drive** or **On directory**, and then select **OK**.

   - If there is no access control profile, a message is displayed prompting you to create one. Select **OK** to create the access profile.

     The Access Control Profile notebook is displayed.
   - If there is an access profile, no message appears. The Access Control Profile notebook is displayed.
10. Complete the pages in the Access Control Profile notebook.
11. Select **Create** or **Set** to close the notebook.

    If it is a directory alias, a message is displayed prompting you whether to propagate the access permissions to all subdirectories in the path. See “Propagating Access Control Profiles to Subdirectories” on page 88 for information about propagating (applying) an access profile to subdirectories.
12. Select **OK** to propagate access to all the subdirectories in the path, giving users Read (R), Write (W), and Create (C) access to the entire program directory tree.

    The alias is created, the resource is shared, and the access control profile is created. An icon representing the alias is added to the Resource Definitions object in the domain.

Creating Access Control Profiles for Resources without Aliases

Use the following steps to grant access permissions for resources that do not have aliases.

To create an access control profile for a shared resource not identified by an alias:

1. Open **LAN Server Administration**.
2. Open the appropriate domain object.
3. Open **Defined Servers**.
4. With mouse button 2, select the appropriate server object.
5. From the pop-up menu, select the arrow to the right of **Open as**.
6. Select the arrow to the right of **Current shares**.
7. Select the type of resource you want to start or stop sharing:
   - **Directories**
   - **Printers**
   - **Serial devices**

   The Current Shares window is displayed. It includes a list of resources defined on the domain for this server as network resources currently shared.
8. Select **Share another**.
9. Type a unique netname in the **Netname** field.
10. Complete the remaining fields.

11. Select **OK**.
12. If you want to create or revise an access control profile for this resource, select it from the list and then select **Manage access** in the Current Shares window.

    Directory resources require an access control profile before users can use them.

    - If there is no access control profile, a message is displayed prompting you to create one. Select **OK** to create the access profile.

      The Identity page of the Access Control Profile notebook is displayed.
    - If there is an access profile, no message appears. The Identity page of the Access Control Profile notebook is displayed.

    An access control profile can be inherited automatically if the directory resource is either created remotely or resides on an HPFS or JFS drive and the 386 HPFS is installed on the server. Even if an access profile is inherited, you may still need to modify the permissions. If the alias is a directory alias, a message is displayed to determine if you want to propagate the access down the directory tree. Directory resources require an access control profile before users can use them.

    The Access Control Profile notebook is displayed. It provides information about the name of the access control profile.
13. Select the **Permissions** tab.

    The Permissions page is displayed. It displays the current access permissions for this resource.
14. Select **Add**.

    The Add Access Control Entries window is displayed.
15. Select the names of the user IDs and groups that you want to give access to this resource.
16. Select the permissions to give them.
17. Select **OK**.
18. Select **Set** or **Create** to close the Access Control Profile notebook.

    If you are giving access to a directory resource, the Propagate Access Profile to Subdirectories message is displayed.
19. If you want to propagate this access control profile to this resource to all subdirectories, select **OK**. If not, select **Cancel**.
20. Select **Close** to close the Current Shares window.

Updating an Access Control Profile

The following are two ways to update an access control profile:

- At the OS/2 command prompt, using the NET ACCESS command. Refer to the *Command Reference*.
- Through LAN Server Administration, for resources with and without aliases. The following information describes this method.

If you rename a directory, you must manually delete and recreate any access control profiles for subdirectories under the directory. Renaming a directory in the HPFS, FAT, or JFS file system does not automatically update access control profiles for the subdirectories. The 386 HPFS access control profiles remain with the renamed directory.

Note: Only an administrator or an operator or user with P permission can modify an access control profile.

For more information, see the following topics:

- "Updating Access Control Profiles for Resources with Aliases"
- "Resources without Aliases" on page 95

Updating Access Control Profiles for Resources with Aliases

Use the following procedure for resources with aliases.

To update an access control profile for a resource identified by an alias:

1. Open **LAN Server Administration**.
2. Open the domain object in which you want to update the access control profile.
3. Open the appropriate Resource Definitions folder.
4. With mouse button 2, select the appropriate alias object.
5. From the pop-up menu, select **Manage access**.

   Note: If you create more than two serial device aliases, you should increase the values of the **maxchdevq** and **maxchdevs** parameters in the IBMLAN.INI file.

   The Access Control Profile notebook is displayed. It provides information about the name of the access control profile.
6. If you want to update access permissions, select the **Permissions** tab.

   You can add user or group IDs, change permissions for an entry, and remove an entry:
   - **To add user or group IDs**:
     a. Select **Add**.
     b. Select one or more names and their permissions.
     c. Select **OK**.
   - **To change permissions**:
     a. Select the name of the user or group for which you want to change access permissions.
     b. As appropriate for your needs, select **Replace**, **Add**, or **Remove**.
     c. In the **Change Permissions** list, select the permissions you want to substitute, add, or remove. Select **Refresh** if you want to undo your selections.
     d. Select **Change**.
   - **To remove user or group IDs from the access control profile:**
     a. Select one or more names from the list.
     b. Select **Remove**.
     c. Select **OK** on the confirmation window.
7. If you want to change the auditing for this access control profile:
   a. Select the **Auditing** tab.
   b. Select one of the audit levels.
8. Select **Set**.

Resources without Aliases

Use the following procedure for resources without aliases.

To update an access control profile of a resource not identified by an alias:

1. Open **LAN Server Administration**.
2. Open the appropriate domain object.
3. Open **Defined Servers**.
4. With mouse button 2, select the appropriate server object.
5. From the pop-up menu, select the arrow to the right of **Open as**.
6. Select the arrow to the right of **Current shares**.
7. Select the type of resource you want to start or stop sharing:
   - **Directories**
   - **Printers**
   - **Serial devices**

   A Current Shares window is displayed. It includes a list of resources defined on the domain for this server as network resources currently shared.
8. Select the resource for which you want to update access control.
9. Select **Manage access**.

   Note: If you create more than two serial device aliases, increase the values of the **maxchdevq** and **maxchdevs** parameters in the IBMLAN.INI file.

   The Access Control Profile notebook is displayed. It provides information about the name of the access control profile.
10. If you want to update access permissions, select the **Permissions** tab.

    You can add user or group IDs, change permissions for an entry, and remove an entry:
    - **To add user or group IDs**:
      a. Select **Add**.
      b. Select one or more names and their permissions.
      c. Select **OK**.
    - **To change permissions**:
      a. Select the name of the user or group for which you want to change access permissions.
      b. As appropriate for your needs, select **Replace**, **Add**, or **Remove**.
      c. In the **Change Permissions** list, select the permissions you want to substitute, add, or remove. Select **Refresh** if you want to undo your selections.
      d. Select **Change**.
    - **To remove user or group IDs from the access control profile:**
      a. Select one or more names from the list.
      b. Select **Remove**.
      c. Select **OK** on the confirmation window.
11. If you want to change the auditing for this access control profile:
    a. Select the **Auditing** tab.
    b. Select one of the audit levels.

12. Select **Set**.

Deleting an Access Control Profile

There are three ways to delete access control profiles:

- At the OS/2 command prompt, using the NET ACCESS command. Refer to the *Command Reference*.
- Using a redirected drive. When you delete a directory while in a redirected drive, if the directory resource associated with the drive is protected by a profile, the profile is also deleted.
- Through LAN Server Administration, for resources with and without aliases. The following information describes this method.

If you delete a directory on a *local drive*, the associated access control profile is not deleted. However, if you delete a directory on a *local 386 HPFS drive*, the access control profile is deleted. If you delete the directory of a *redirected drive*, the access control profile is always deleted, whether it is on a local 386 HPFS drive or not. Check the access control profiles on each server periodically, and delete those that have no existing directory resource.

Attention: After you delete an access control profile, you cannot recover it.

For more information, see the following topics:

- "Resources with Aliases"
- "Resources without Aliases"

Resources with Aliases

Use the next procedure to delete the access control profile for an alias.

Regardless of how many aliases are defined for a resource, only one access control profile exists for a resource. When you complete the following procedure, the access control profile for this resource (and consequently, for all its aliases) is deleted.

To delete access control for an alias:

1. Open **LAN Server Administration**.
2. Open the domain object for the aliased resource.
3. Open the appropriate Resource Definitions folder.
4. Open the appropriate alias object.

   The alias notebook is displayed.
5. Select **Manage access**.

   The Access Control Profile notebook is displayed. It provides information about the name of the access control profile.
6. Select **Delete**.

Resources without Aliases

You should periodically delete access control profiles for resources that are not identified by an alias to ensure that access profiles for nonexistent directories are deleted. If a directory resource (such as C:\TESTDIR1 on SERVER1) is protected by an access profile, and if that resource is deleted from the SERVER1 hard disk, the access control profile associated with that resource is not deleted. Use the following steps to delete the access control profiles associated with that resource. The BACKACC and RESTACC utilities also can be used to delete access control profiles for nonexistent directories.

To delete access control for a resource without an alias:

1. Open **LAN Server Administration**.
2. Open the appropriate domain object.
3. Open **Defined Servers**.
4. With mouse button 2, select the appropriate server object.
5. From the pop-up menu, select the arrow to the right of **Open as**.
6. Select the arrow to the right of **Current shares**.
7. Select the type of resource you want to start or stop sharing:
   - **Directories**
   - **Printers**
   - **Serial devices**

   The Current Shares window is displayed. It includes a list of resources defined on the domain for this resource as network resources currently shared.
8. Select the resource for which you want to delete access control.
9. Select **Manage access**.

   The Access Control Profile notebook is displayed. It provides information about the name of the access control profile.
10. Select **Delete**.

Default Access Control Profiles on Servers

The following profiles contain the default access control profiles for servers. These access control profiles allow the server to operate properly while providing only minimal access to important files. Changing these access control profiles may affect such functions as server startup and user logon assignments and applications.

In addition to providing default access control profiles on the server, an access control profile providing all permissions is assigned to each user who has a home directory. The access control profile is added to the server and path assignment specified during the creation of the home directory.

The default auditing controls for the profiles added by the Server and DLRinst services are set to log an audit record only in the event of failures. You may want to change the auditing controls on the access control profiles to improve network monitoring and maintenance.

The following access control profiles are the default profiles added at the domain controller when the Server service is started:

```
d:\IBMLAN\DCDB          GUESTS:R  USERS:R
d:\IBMLAN\DCDB\APPS     GUESTS:R  USERS:R
d:\IBMLAN\DCDB\DATA     GUESTS:R  USERS:R
d:\IBMLAN\DCDB\DEVICES  GUESTS:R  USERS:R
d:\IBMLAN\DCDB\FILES    GUESTS:R  USERS:R
d:\IBMLAN\DCDB\LISTS    GUESTS:R  USERS:R
d:\IBMLAN\DCDB\PRINTERS GUESTS:R  USERS:R
d:\IBMLAN\NETPROG       GUESTS:R  USERS:R
d:\IBMLAN\BOOK          GUESTS:R  USERS:R
```

where *d* is the drive where the IBMLAN directory is located.

The following access control profiles are the default profiles added at all servers when the Server service is started:

```
d:\IBMLAN\DOSLAN\NET   GUESTS:R   USERS:R
d:\IBMLAN\DOSLAN\DOS   GUESTS:R   USERS:R
d:\IBMLAN\DCDB\IMAGES  GUESTS:R   USERS:R
\PIPE\IBMLAN\SERVER.RNS               GUESTS:RW  USERS:RW
```

where *d* is the drive where the IBMLAN directory is located.

The following access control profiles are added at the domain controller when the DLRinst service is started:

```
d:\IBMLAN\DOSLAN\DLRINST        GUESTS:R     USERS:R
d:\IBMLAN\DOSLAN\LSP            GUESTS:R     USERS:R
C:\PCLP13XS\BATCH               GUESTS:R     USERS:R
C:\PCLP13XS\LISTS               GUESTS:R     USERS:R
C:\PCLP13XS\USERS               GUESTS:RWCD  USERS:RWCD
C:\PCLP13XS\USERS\PCLP          GUESTS:R     USERS:R
```

DBCS Note: The preceding access control profiles do not propagate to DBCS systems. For DBCS systems, the following access control profiles are the default profiles added at all servers when the Server service is started:

```
d:\IBMLAN\DOSLAN\NET             GUESTS:R   USERS:R
d:\IBMLAN\DOSLAN\DOS             GUESTS:R   USERS:R
d:\IBMLAN\DCDB\IMAGES            GUESTS:R   USERS:R
-PIPE\IBMLAN\SERVER.RNS          GUESTS:RW  USERS:RW
```

The NetLogon service on all servers adds an access control profile of USERS:RX and ADMINS:RX for the path specified by the **scripts** parameter in the NetLogon section of the IBMLAN.INI file.

The following access control profiles are added for each user’s DCDB directory:

```
d:\IBMLAN\DCDB\USERS\userid userid:RWCXDAP
d:\IBMLAN\DCDB\USERS\userid\BATCH userid:RWCXDAP
```

The following access control profiles are added to servers when the Server service is started, the remote IPL service is installed, and GETRPL has been run:

```
d:\IBMLAN\RPL  RPLGROUP:RX
d:\IBMLAN\RPL\OS2  RPLGROUP:RX
d:\IBMLAN\RPL\OS2\SYSTEM  RPLGROUP:RX
d:\IBMLAN\RPL\IBMLAN  RPLGROUP:RX
d:\IBMLAN\RPL\IBMLAN\NETLIB  RPLGROUP:RX
d:\IBMLAN\RPL\IBMLAN\NETPROG  RPLGROUP:RX
d:\IBMLAN\RPL\IBMLAN\SERVICES  RPLGROUP:RX
d:\IBMLAN\RPL\IBMCOM  RPLGROUP:RX
d:\IBMLAN\RPL\IBMCOM\DLL  RPLGROUP:RX
d:\IBMLAN\RPL\IBMCOM\MACS  RPLGROUP:RX
d:\IBMLAN\RPL\MUGLIB  RPLGROUP:RX
d:\IBMLAN\RPL\DOS  RPLGROUP:RX
d:\IBMLAN\RPL\FITS  RPLGROUP:RX
d:\IBMLAN\RPLUSER
d:\IBMLAN\RPLUSER\DEFALT20
d:\IBMLAN\RPLUSER\DEFALT20\IBMCOM
d:\IBMLAN\RPLUSER\DEFALT20\IBMLAN
d:\IBMLAN\RPLUSER\DEFALT20\OS2
d:\IBMLAN\RPLUSER\DEFALT20\OS2\SYSTEM
d:\IBMLAN\RPLUSER\DEFALT20\SPOOL
d:\IBMLAN\DICTIONA
```

where *d* is the drive where the IBMLAN directory is located.

The following access control profiles are added to servers when Local Security is installed:

For all subdirectories specified by the DPATH environment variable	LOCAL:RX
For all subdirectories specified by the PATH environment variable	LOCAL:RX
For all subdirectories specified by the LIBPATH variable in CONFIG.SYS	LOCAL:RX
For all subdirectories specified by the DESKTOP directory tree	LOCAL:RWX
For all subdirectories specified by the GLOSSARY environment variable	LOCAL:RX
For all subdirectories specified by the BOOKSHELF environment variable	LOCAL:RX
For the file referenced by the USER_INI environment variable	LOCAL:RWX
For the file referenced by the SYSTEM_INI environment variable	LOCAL:RWX
For all subdirectories specified by the TMP environment variable	LOCAL:RWXCD
For all subdirectories specified by the TEMP environment variable	LOCAL:RWXCD
x:\	LOCAL:RX
Other HPFS drive roots	LOCAL:RX
x:\OS2	LOCAL:RX
x:\IBM386FS	LOCAL:RX
x:\OS2\INSTALL	LOCAL:RX
x:\OS2\HELP	LOCAL:RX

DBCS Note: The following access control profile is added only for DBCS systems:

x:\OS2\SYSDATA	LOCAL:RWX

x:\OS2\BOOK	LOCAL:RX
x:\OS2\DLL	LOCAL:RX
x:\OS2\SYSTEM	LOCAL:RX
x:\SPOOL and subdirectories (queues)	LOCAL:RWXCDA
x:\IBMCOM	LOCAL:RX
d:\IBMLAN	LOCAL:RX
d:\IBMLAN\BOOK	LOCAL:RX
d:\IBMLAN\ACCOUNTS	LOCAL:RX
d:\IBMLAN\LOGS	LOCAL:RX
d:\IBMLAN\ACCOUNTS\NET.ACC	LOCAL:RWX
d:\IBMLAN\ACCOUNTS\NETACC.BKP	LOCAL:NONE
d:\IBMLAN\NETLIB	LOCAL:RX
d:\IBMLAN\NETPROG	LOCAL:RX
x:\IBM386FS\HPFS386.IFS	LOCAL:NONE
d:\IBMLAN\INSTALL	LOCAL:NONE
d:\IBMLAN\SERVICES	LOCAL:RX
x:\MUGLIB	LOCAL:RX
x:\MUGLIB\ACCOUNTS	LOCAL:RX
x:\MUGLIB\DLL	LOCAL:RX
x:\OS2\MDOS\WINOS2\SYSTEM	LOCAL:RX
x:\OS2\MDOS\WINOS2\*.INI	LOCAL:RWX
x:\OS2\MDOS\WINOS2\*.GRP	LOCAL:RWX
x:\NOWHERE	LOCAL:RWX

where *x* is the drive from which OS/2 was started and *d* is the drive where the subdirectory is located.

Notes:

1. The default access control profiles for Local Security permit the default OS/2 Desktop to start for users and if no one is logged on. If the Desktop has been reconfigured, not all of the correct access control profiles may have been

created. If the Desktop cannot be started when no one logs on, try logging on as an administrator. Then verify that all of the objects referred to during the Desktop initialization are displayed correctly.

2. The DESKTOP and NOWHERE directory names may be different on other machines. For example, the OS/2 Desktop may have been renamed to MYDESKTOP. In this case, MYDESKTOP should have LOCAL:RWX access. The NOWHERE directory name is translated for different languages.

CD-ROM Devices and Access Control Profiles

OS/2 Warp Server or LAN Server periodically checks for the existence of a directory resource protected by an access control profile. Therefore, it is important that you correctly define access control profiles for removable SCSI devices such as CD-ROM devices. Otherwise, you may get a missing files message because the access control profile has filtered out unknown directories and files. Users may not be able to access data on a CD-ROM between different media insertions.

For example, if you use the IBM Enhanced CD-ROM II device locally on an IBM server as the I drive, ensure that the access control profile specifies the I drive, not the I directory, as the shared resource. In this way, all files on any CD are available when shared over the LAN. Otherwise, only directories and files from the specific CD that was used when the access control profile was created are visible to LAN clients. In this case, you can issue the following command when logged on the LAN as an administrator: `NET ACCESS I: /ADD USERS:RWCD`

Chapter 8. Limiting Space within Directories on 386 HPFS Servers

This chapter discusses directory limits, or disk space allocation, for use with the OS/2 Warp Server and LAN Server programs when running 386 HPFS. Directory limits provide management of disk space at the directory level on servers.

The allocation scheme works in the same way as the partition of a logical drive. When a directory tree is full, no user can append data to its files or create subdirectories within the tree. For example, a limit of 100MB applied to the C:\IBMLAN directory allows only those requests for disk space that do not cause the usage count to exceed 100MB.

This chapter also discusses a notification function, which you can use to set up alerts to notify selected users when a directory tree is either full or is nearing its maximum capacity.

For more information, see the following topics:

Definition of Terms

This chapter contains the following specialized terms:

Available space
The amount of free disk space within a particular directory tree. The available space is the limit minus the usage count. However, the available space for a directory tree can be affected by limits placed above the directory itself. Consider this example:

- Root directory C:\ has a limit of 250MB. Its usage count is 200MB.
- Directory C:\IBMLAN has a limit of 100MB. Its usage count is 20MB.
- The available space for the root directory is 50MB, which is also the available space for the C:\IBMLAN directory because C:\ is in the same path as C:\IBMLAN. Without the limit on C:\, the available space at C:\IBMLAN is either 80MB or the free space of the drive, whichever is less.

Drive
A logical drive, used interchangeably with *volume*.

Limit
A value, in kilobytes (KB), used to control the size of a directory tree.

Threshold alert
An alert generated when the size of a limited directory increases past a size threshold, a set percentage of the directory limit.

Threshold delay
The minimum amount of set time that must elapse before the crossing of the same or lower threshold (percentage of limit) can generate another threshold alert.

Usage count The current size of the directory tree as specified in KB.

Volume A logical drive, used interchangeably with *drive*.

How Directory Limits Work

You apply directory limits only to directories, not to files. The limit you set on a directory applies to all users who have access to that directory. No distinction is made between users.

By combining directory limits with the access control profiles of OS/2 Warp Server or LAN Server, you can control both the access to a directory and the size of that directory. For example, you can give user JOE read, write, create, or delete access to the C:\IBMLAN\USERS\JOE directory and a limit of 20MB for his own use.

The following topics include important principles of operation for directory limits.

- “Application, Hierarchy, and Number Rules”
- “Independence”
- “Privileged Processes Not Limited” on page 103
- “Enabling and Removing” on page 103
- “Obtaining Information” on page 103
- “Tasks of Users and Administrators” on page 103
- “What Disk Space Includes” on page 104

Application, Hierarchy, and Number Rules

The following rules apply to directory limits:

- You can apply limits only to directories, not to files.
- Limits are hierarchical. A limit on a directory controls the entire subtree below the directory itself. For example, a limit on the root directory controls the whole drive.
- You can place multiple limits within a path. For example, you can place a limit at the root directory and another at the C:\IBMLAN directory.

Independence

OS/2 Warp Server and LAN Server use directory limits when a request for disk space is received. For a request to be granted, it must satisfy all the limits placed within its path. What this means is that although directory limits can be set independently of each other, the limit set on a directory can also affect its subdirectory.

For example, you can set a limit of 100MB at the C:\ directory and another limit of 120MB at the C:\IBMLAN directory. In this example, although you set a limit of 120MB for the C:\IBMLAN directory, the size of that directory is also limited by the

100MB limit you set on its parent directory (C:\). Consequently, a disk space request larger than 100MB to the C:\IBMLAN directory would be denied.

Privileged Processes Not Limited

Limits are not enforced for privileged processes. Privileged processes are:

- All processes (local and from clients) initiated by an administrator. That is, administrators are not subject to limits.
- Privileged local processes when Local Security is installed.
- All local processes when Local Security is not installed.

Enabling and Removing

Directory limits are part of 386 HPFS. You can enable this function on, or disable it from, any 386 HPFS drive.

Note: Previous versions of 386 HPFS and HPFS.IFS cannot access drives that have directory limits enabled on them. You must create a new 386 HPFS Startup diskette. For information on making utility/startup diskettes, refer to the *Command Reference*.

Obtaining Information

You can obtain information about limits if you have access to the directory in which you are interested and you specify the DIR command on that directory to display its content. If you do not have access, the contents of the directory are not displayed. Because the DosQFSInfo( ) call is a volume-based API, the DIR command always reports the amount of free space on the drive. It is not subject to directory limits.

Tasks of Users and Administrators

Users who are also administrators can modify directory limits at will.

Users who are not administrators can manage the limit of a directory if they are given P permission on the parent of the target directory itself. For example, assume that user ID JOHN has RWCDXAP permissions on the C:\IBMLAN\USERS\JOHN directory. JOHN can create the directory C:\IBMLAN\USERS\JOHN\PUBLIC and apply a limit of 15MB to it. However, he cannot modify the limit placed on directory C:\IBMLAN\USERS\JOHN directory unless he has P permission for the C:\IBMLAN\USERS directory. John is still subject to directory limits because he is not an administrator.

Consider the following scenario:

The administrator creates a home directory for user ID MARY and gives MARY the permissions RWCDXAP permissions. With these permissions, MARY can control access by other user IDs to her home directory.

The administrator also sets a limit of 100MB on the home directory. MARY can now administer her home directory for access control and disk usage. MARY creates a directory called PUBLIC within her home directory, applies a limit of 20MB to it and, using the following command, gives unrestricted access to all user IDs:

```
NET ACCESS homedir\PUBLIC /ADD GUESTS:RWCDAX
```

where *homedir* is Mary's home directory.

However, MARY cannot modify the limit (100MB) applied to the root of her home directory.

What Disk Space Includes

Disk space includes all space required to store data on disk. Each directory requires disk space for both the data stored within the directory and the file-system instructions that manage the data. For example, creating a new directory uses 2560 bytes because that much disk space is required to maintain a directory object. Even an empty file (zero bytes) use 512 bytes of disk space. If a directory has 10MB of free disk space, you cannot create a new 10MB file in that directory because the system requires extra space for directory management.

In rare conditions, 386 HPFS does not account for certain file-system structures. These exceptions help 386 HPFS to maintain high performance and have minimal effect on the accounting mechanism.

In certain cases, 386 HPFS allows a limit to be exceeded. These exception occur only when the directory has room for the data that must be written to disk but not for the required file-system structures. For example, consider a directory with 1024 bytes left. A write request of 1024 bytes is made. However, the disk is so fragmented that a file-system structure requiring 512 bytes is needed to manage the data written to disk. In this example, 386 HPFS allows the request to continue and updates the usage count of the directory to reflect the overflow. 386 HPFS denies subsequent requests for disk space.

Enabling Directory Limits on a 386 HPFS Volume

Directory limits, by default, are not activated on a particular volume. You can enable this function on a drive from LAN Server Administration, the command line, or the NetDASDCtl() application programming interface (API). However, before using any method, be aware of the following:

- When you issue the ENABLE command, 386 HPFS first calculates the size of each directory in the tree. To accomplish this, 386 HPFS processes the entire directory tree and the files contained within it.
- If you are attempting to enable directory limits on the boot drive, the process is only partially completed. 386 HPFS is not able to lock the drive because OS/2 always keeps certain files open. This failure also can occur on other drives that have open files. A shutdown of your system followed by a restart completes the activation process.
- If the CHKDSK command repairs a drive on which directory limits are active, 386 HPFS recalculates the size of each directory. This action is necessary because the CHKDSK command, as part of its repair operation, moves files and directories. For example, it creates the FOUND.000 and DIR0000.CHK files.
- Drives on which directory limits are enabled are inaccessible to HPFS.IFS and earlier versions of 386 HPFS (for example, LAN Server 2.0 and 3.0). You must create a new startup 386 HPFS diskette if you choose to use this function. Otherwise, you cannot access these volumes when starting from a diskette.

To enable directory limits on a volume:

1. Open **LAN Server Administration**.

2. With mouse button 2, select the **Local Workstation**.
3. From the pop-up menu, select the arrow to the right of **Open as**.
4. Select **Current shares**.
5. Select **Directories**.

   The Current Shares window is displayed. It includes a list of directory resources currently shared.
6. Select the resource for which you want to enable directory limits.
7. Select **Manage limits**.
8. If directory limits have not been enabled for the resource you selected, you are prompted whether you want to enable limits. Select **Yes**.
9. If the drive you are attempting to enable is already being used by another process, a message is displayed instructing you to restart your workstation to complete the enabling process. After you restart your workstation, go to "Limiting a Directory".
10. If the drive you are trying to enable is not being used by another process, the Directory Limits window is displayed.

    Specify the limit for the selected directory.

Note: You can also enable directory limits using the NET DASD command. For more information, see the *Command Reference*.

To incorporate directory limits within your own applications, use the NetDASDCtl() API provided. For information on how to do this, see the *Programming Guide and Reference* .

Limiting a Directory

After you have enabled directory limits on a volume, you can view or change limits to directories on that volume. The following steps are performed at the server for which you are enforcing directory limits.

Note: A network administrator can manage directory limits on a local or remote server. A user with server operator privilege can manage a local server. Managing directory limits on a local server is preferred because the procedure can be time consuming.

To set a limit for a directory:

1. Open **LAN Server Administration**.
2. With mouse button 2, select the **Local Workstation** or the appropriate server object.
3. From the pop-up menu, select the arrow to the right of **Open as**.
4. Select **Current shares**.
5. Select **Directories**.

   The Current Shares window is displayed. It includes a list of directory resources currently shared.
6. Select the resource for which you want to set directory limits.
7. Select **Manage limits**.
8. If directory limits has not been enabled for the resource you selected, you are prompted whether you want to enable limits. Select **Yes**.

   The Directory Limits window is displayed.

9. Select one of the following units of measure to indicate the size that this directory is allow to fill before a directory-full alert is sent out:
   - **No limit**
   - **Specify in kilobytes**
   - **Specify in megabytes**
10. Specify the **Alert threshold** and **Alert increment** if desired. (For more information, see "Directory-Specific Settings for Alerts" on page 109)
11. Select **OK**.

Note: You can also enable directory limits using the NET DASD command. For more information, see the *Command Reference*.

Alerts for Directory Limits

When limits are set on the size of a directory or tree, the users of that directory cannot exceed the limit. Therefore, you should notify the appropriate people, not only when the directory is full, but as it increases to the point (threshold) that it might not hold the necessary files.

After the threshold is reached, the directory can decrease or increase in size over an unpredictable time span. Administrators and other users appreciate being alerted on a timely basis as the directory approaches and crosses the threshold.

The following example of a threshold alert notifies users of the remaining directory space in a particular directory:

```
Directory MYDIR has crossed a threshold.  The available space in
directory tree is 5KB.
```

The following message is an example of a directory-full alert:

```
There was not enough space within the directory tree
to satisfy your request.  Contact your network
administrator if you need more space.
```

For more information, see the following topics:

- "Threshold Alerts"
- "Directory-Full Alerts" on page 107
- "The Two Stages of Setting Alerts" on page 108
- "Directory-Specific Settings for Alerts" on page 109
- "Volume-Wide Settings for Alerts" on page 110

Threshold Alerts

Threshold alerts are posted when one percentage threshold is reached as the disk space for the directory increases within the set limit. The following figure illustrates the threshold, the limit, and their relationship to directory size.

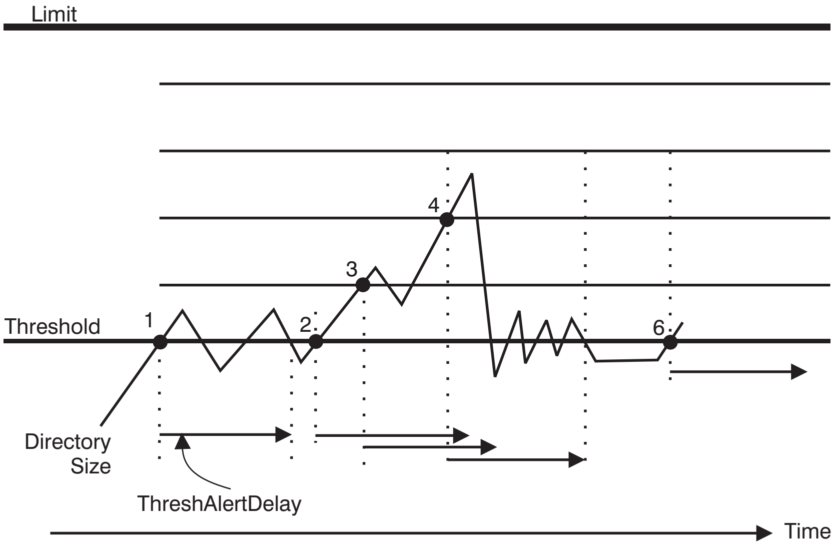


Figure 2. Threshold Alerts

As the size of the directory increases, it crosses the threshold (1) and generates an alert. You can divide the threshold into *incremental thresholds*, which, as they are crossed, post additional threshold alerts.

The **ThreshAlertDelay** parameter in the HPFS386.INI file defines the threshold delay, or the minimum amount of time that must elapse before another crossing of the same or lesser threshold generates an alert (2 and 6). (The same threshold or a lesser one can be crossed when the size of the directory decreases.) The threshold delay is overridden when the directory size crosses a higher threshold (3 and 4).

Directory-Full Alerts

Directory-full alerts are posted when a directory tree is full. The following figure illustrates the relationship between alerts, directory limits, and directory sizes.

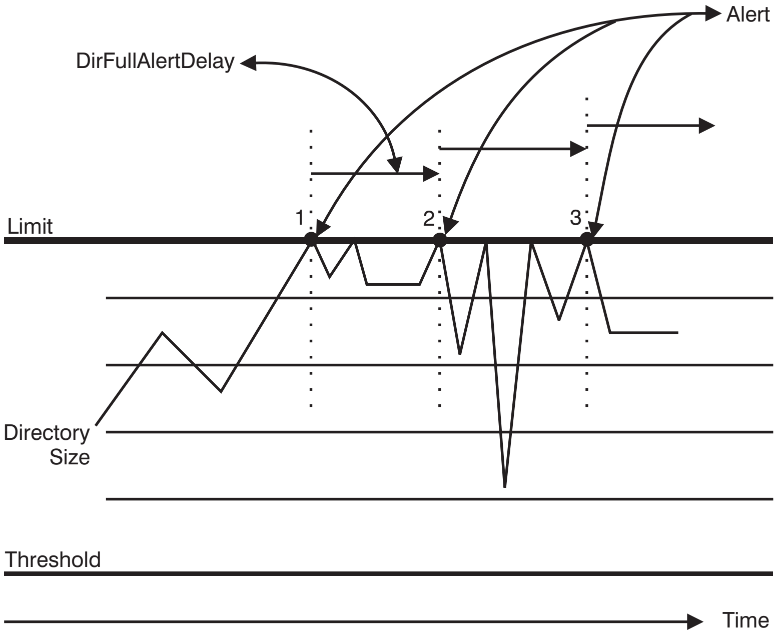


Figure 3. Directory-Full Alerts

Because the user cannot cross the directory limit, directory-full alerts are generated only when a directory-full condition is reached. A directory-full condition occurs when a write request is denied because of insufficient space within the directory tree. Like threshold alerts, directory-full alerts have a delay window that allows you to control alert notification. The delay is provided by the **DirFullAlertDelay** parameter in the HPFS386.INI file, which defines the minimum amount of time that must elapse before another directory-full condition generates an alert (2 and 3). The delay prevents alerts from being generated in quick succession when the directory space rapidly fluctuates between the limit and a lower value.

The Two Stages of Setting Alerts

You set up alerts in two stages:

- Make directory-specific settings for alerts. You make these settings for the threshold value and the incremental threshold values. These settings apply only to the directory you specify.
- Set volume-wide settings for alerts. Set these settings in the HPFS386.INI file or a *filename*.INI file (where *filename* is a name of your choosing) on the IFS= line of the file by changing the values of the supplied parameters. Parameter values control the following variables:
  - Who receives alerts
  - Whether the user who caused the alert receives it
  - Delay time that must elapse before another alert of the same type is generated after the crossing of the same or lower threshold or directory-full condition

Although you can perform either stage first, it usually is more logical to begin with volume-wide settings.

Directory-Specific Settings for Alerts

Use the following procedure to set directory-specific alerts.

To set directory-specific alerts:

1. Open **LAN Server Administration**.
2. Open the appropriate domain object.
3. With mouse button 2, select the **Local Workstation** or the appropriate server object.
4. From the pop-up menu, select the arrow to the right of **Open as**.
5. Select **Current shares**.
6. Select **Directories**.

   The Current Shares window is displayed. It includes a list of directory resources currently shared.
7. Select the resource for which you want to set directory-specific alerts.
8. Select **Manage limits**.
9. If directory limits has not been enabled for the resource you selected, you are prompted whether you want to enable limits. Select **Yes**.
10. If the drive you are attempting to enable is already being used by another process, a message is displayed instructing you to restart your workstation to complete the enabling process. After you restart your workstation, return to either step 1 or 2.
11. If the drive you are trying to enable is not being used by another process, the Directory Limits window is displayed.
12. Select **Specify threshold**, and set the threshold value.

    The threshold value is a percentage of the set directory limit. The valid range is 1 to 99. An alert is posted when the directory is this percentage full.
13. Select **Specify increment**, and set the incremental threshold value.

    The incremental threshold value is a percentage of the set directory limit. Valid ranges are values less than or equal to (100 - threshold value - 1). An alert is generated each time the directory increases by this incremental value after the threshold is reached.

    Note: For example, if you specified a directory limit of 1000KB, a threshold of 80 percent, and an increment value of 3 percent, the following happens:

    - The first threshold alert is posted when the directory increases to 80 percent (800KB) of its limit (1000KB).
    - From that point, each time the directory increases 3 percent (30KB) of the directory limit, another threshold alert is posted. Threshold alerts are posted as the directory grows to the following sizes: 800, 830, 860, 890, 920, 950, and 980.
    - A directory-full alert is posted at the limit of 1000KB.
14. Select **OK**.

You can also set directory-specific alerts limits using the NET DASD command. For more information, see the *Command Reference*.

Volume-Wide Settings for Alerts

You control settings for volume-wide alerts with parameters that you set in the HPFS386.INI file. The values for these parameters become active when you restart the server.

The list below describes the volume-wide parameters stored in the HPFS386.INI file (or an .INI file you created). Some parameters control who receives alerts; others control the delay value.

Parameter **Description**

DirFullAlertNames
Specifies, on a per-volume basis, the user or group IDs to receive alerts when the size of a directory has reached the set limit.

DirFullAlertUser
Specifies whether a user ID that encounters a directory-full condition receives an alert. Specify either `Yes` or `No`.

ThreshAlertNames
Specifies the user IDs to receive alerts when a threshold is exceeded.

ThreshAlertUser
Specifies whether a user ID that caused a threshold to be crossed requires notification. Specify either `Yes` or `No`.

DirFullAlertDelay
Defines, in minutes, the ThreshDelay period for directory-full conditions.

ThreshAlertDelay
Defines, in minutes, the ThreshDelay period for the threshold crossing.

For more information, see the following topics:

- "Format of Parameter Values"
- "Setting Parameter Values" on page 111

Format of Parameter Values

The HPFS386.INI file stores volume-wide information patterned after the following format:

< *parameter*>=< *drive letters*>: *arg1 arg2 ... argN*

where:

parameter Specifies the parameter in the DASD_Limits section of the HPFS386.INI file.

drive letters Specifies the drives to which the parameter applies.

arg1 arg2 ... argN
Specifies the variable number of arguments to apply to this use of the parameter. Depending upon the parameter, arguments can be the name of subdirectories, user IDs, "Yes" or "No", or a numerical value for minutes.

Several rules apply to the HPFS386.INI file:

- When used instead of drive letters, the * (asterisk) denotes all 386 HPFS drives.
- If the same parameter is specified with the same drives more than once, the occurrence positioned lower in the file overrides the previous occurrence.
- To add comment lines in the file, comment them out with semicolons as shown in the following example.

The following example shows the parameters are located under the DASD_Limits section of the HPFS386.INI file.

Note: The * (asterisk) wildcard character signifies all 386 HPFS drives.

```
[DASD_Limits]


ThreshAlertNames=*:userid1 userid2 groupid4   ;For all 386 HPFS drives
ThreshAlertDelay=CDE: 60           ;1 hour delay for drives C, D, E
ThreshAlertDelay=FG: 10            ;Delay for drives F and G
ThreshAlertUser=DE: Yes            ;Notify user by sending
                                   ;a message.


DirFullAlert Names=CDE: admins ;Notify all administrators
DirFullAlertDelay=*: 5             ;Post alerts no less than
                                   ;5 minutes apart
DirFullAlertUser=DEG: Yes          ;Notify user who requested space
DirFullAlertUser=C: No             ;No alerts to any user for drive C
```

For more information, see the following topic:

- “Parameter Default Values”

Parameter Default Values: Parameters have the following default values if you do not specify other values:

Parameters **Default Values**

ThreshAlertNames and DirFullAlertNames
ADMINS

ThreshAlertDelay and DirFullAlertDelay
10 minutes

ThreshAlertUser and DirFullAlertUser
Yes

Setting Parameter Values

Use the following procedures to set parameters for directory limits.

To set directory limits parameters:

1. Open the 386 HPFS initialization file in the IBM386FS directory. This file contains the directory limits parameters.
2. Set any of the parameter values as needed to configure your alerts for directory limits.
3. Stop the server using the Shutdown command, and then start it again to enable the changes.

You can use the same parameters as many times as necessary. The next procedures demonstrate how to set the specific parameter values.

For more information, see the following topic:

- “Specifying Who Receives Alerts Across a Volume”Specifying Who Receives Alerts Across a Volume
- “Specifying if the User Receives the Alerts”Specifying if the User Receives the Alerts
- “Specifying Alert Delay Times”Specifying Alert Delay Times

Specifying Who Receives Alerts Across a Volume: The parameters **DirFullAlertNames** and **ThreshAlertNames** specify the user IDs that receive alerts.

To specify these parameters:

1. Open the 386 HPFS initialization file in the IBM386FS directory, and locate the DASD_Limits section.
2. After the parameter and its equal sign, type either the drive letter affected or an asterisk (*) to specify all 386 HPFS drives. Then type yes or no to receive the type of alert specified by the parameter.
3. Stop the server using the shutdown command, and then start the server again to enable the changes.

Specifying if the User Receives the Alerts: The parameters **DirFullAlertUser** and **ThresAlertUser** specify whether the user who caused one of these types of alerts receives the alert.

To specify these parameters:

1. Open the HPFS386 file in the IBM386FS directory, and locate the DASD_Limits section.
2. After the parameter and its equal sign, type either the drive letter affected or an asterisk (*) to specify all 386 HPFS drives. Then type `Yes` if you want a user to be notified of the event or `No` if not.
3. Stop the server using the shutdown command, and then start the server again to enable the changes.

Specifying Alert Delay Times: With the **DirFullAlertDelay** and **ThreshAlertDelay** parameters, you can specify the amount of time that must elapse before another alert is generated for the same alert condition.

To specify alert delay times:

1. Open the HPFS386.INI file, and locate the DASD_Limits section.
2. After the parameter and its equal sign, type either the drive letter affected or an asterisk (*) to specify all 386 HPFS drives. Then type the number of minutes for delay.

   For example, to set a delay time of 5 minutes for directory-full alerts on all drives and add a comment, type:

   ```
   DirFullAlertDelay=*: 5  ;Post alerts no less than  ;5 minutes apart
   ```
3. Stop the server using the shutdown command; then start the server again to enable the changes.

Chapter 9. Managing OS/2, DOS, WorkSpace On-Demand, and Windows Applications

An *application* is a set of program data files and other files necessary to do a specific job or function, such as word processing. A *network application* is an application that is defined to and usually shared on the network. You define network applications as either public or private. A user finds and starts network applications in a program starter, which varies depending on the user's operating system.

For brevity, this chapter uses *program starter* as a general term to indicate where a user starts public and private applications. The program starter for OS/2 users is the Network Applications folder. The program starter for DOS users depends on whether they run Windows with DOS LAN Services (DLS).

For DLS machines with Windows, the program starter is the **LAN Applications** list, which is in the Application Installation window. For DLS machines without Windows, the program starter is the Run Applications window.

For more information, see the following topics:

- "Types of Network Applications"
- "How Network Applications and Remote Program Execution Differ" on page 114
- "Setting Up an OS/2, DOS, WorkSpace On-Demand, or Windows Network Application" on page 114
- "Managing Network Applications" on page 117
- "OS/2 Applications Using Dynamic Link Libraries" on page 121
- "Stopping Applications at Logoff" on page 122
- "Defining Network Messaging as a Public Application for DOS LAN Requester 3.0 Users" on page 122
- "Preparing to Run Programs Remotely" on page 125

Types of Network Applications

OS/2 Warp Server and LAN Server support two main categories of network applications:

- Public
- Private

A *public application* is available to some or all users on the network. A *private application* is created by a user for personal use and is not available to other users.

Users at OS/2 clients can access public and private applications from the Network Applications folder on their desktops. WorkSpace On-Demand users can access public applications from their desktops. Users at DOS LAN Services clients without Windows can access DOS public and private applications from the Run Applications window. Users at DOS LAN Services clients with Windows can access DOS public applications from the **LAN Applications** list, which is in the Application Installation window. These applications are called *shared applications* on these workstations.

You can set up DOS applications to run as OS/2 public or private applications. OS/2 public and private applications can be either local (on the user's workstation) or remote (on a server). In DOS LAN Services, applications that reside on a user's client are called *local applications*.

Refer to the *DLS and Windows User's Guide* for information on setting up private DOS applications for DOS LAN Services users.

When the Network Applications folder is opened for the first time or when the folder is refreshed, implicit network connections are made by the OS/2 operating system for applications stored on a remote server. The implicit connections are made to determine information about the application objects in the folder. The implicit connection is deleted immediately after a program object is created.

These connections can be affected by the **maxuses** parameter setting for shares associated with the network application. For example, a user who opens the folder for the first time may not get the actual application icon if the connection cannot be made to retrieve the icon from the server because the server is already servicing the maximum number of users indicated by the **maxuses** parameter on the server.

How Network Applications and Remote Program Execution Differ

Network applications reside either on a user's workstation (local) or on a server (remote). Remote public applications are loaded from the server and run at the client. Programs that are run as network applications must be compatible with the operating system running on the client. Programs that are run using *remote program execution* (a program running on a remote server) must be compatible with the operating system running at the server.

Running public applications differs from running remote programs. When a user runs a program remotely, that program resides on a server and actually runs in that server's memory, not in the client's memory. Large programs using standard input, output, and error file handles can run remotely in a server's memory, thereby requiring less memory on the client. Users can interact with the program with command line input. To reduce the amount of memory required on a client machine, run large resource-intensive programs of this type on a remote server.

Setting Up an OS/2, DOS, WorkSpace On-Demand, or Windows Network Application

Use the following steps to set up an OS/2, DOS, or Windows network application located on a server.

To set up a WorkSpace On-Demand, OS/2, or DOS application on a server:

1. Install the application.
2. Create a directory alias for the directory containing the application. Create additional aliases, as needed, for any other network resources required by the application.
3. Assign access permissions for the aliases.
4. Define the application.
5. Customize the application to meet your needs or the needs of your users.
6. Add the application for users.

For more information, see the following topics:

- “Installing the Application”
- “Creating Aliases”
- “Assigning Access Permissions” on page 116
- “Defining the Application” on page 116
- “Customizing Applications” on page 117

Installing the Application

Install the application using the instructions that came with the application. Look for requirements specific to the application. For example, some applications are not network-aware. Such applications do not recognize drive letters above E and ports above LPT3 and COM3. Or, an application may search for data files only on drive C or the drive where it was installed.

Note: For WorkSpace On-Demand, the procedure for installing applications is different. See the *WorkSpace On-Demand 2.0 Administrator’s Guide* for more information.

Network-aware applications are applications that use network resources and are designed to be run on a network. *Stand-alone applications*, on the other hand, are designed to be stored and run on the local workstation and are not network-aware. Some restrictions apply when running stand-alone applications on a network.

Install the application in a directory. During installation of some applications, that directory is created for you. Check the documentation that came with the application.

If the application is to be shared among many users, consider installing it in a server’s directory, rather than on a user’s local workstation. (The application is then loaded into the user’s workstation’s memory as needed.) However, if the application searches for data only on drive C, install the application or the data files on the users’ workstations.

If you use server storage for an OS/2 application that includes files with a .DLL extension, you must provide access to those files from any clients that run the application.

Creating Aliases

If you have not already done so, create a directory alias for the directory in which your public application resides and create aliases for other resources required by this application. See “Chapter 6. Sharing Network Resources” on page 65 for more information.

When creating an alias, use the **Maximum concurrent connections** field to limit the number of users accessing the application at the same time. For example, if you bought 10 licenses for this application, specify 10 in that field.

Assigning Access Permissions

If you have not already done so, create an access control profile for the alias and assign access permissions for this alias to users and groups. See “Chapter 7. Defining Access Control Profiles” on page 83 for more information.

Execute (X) permission is usually insufficient for an application to run properly. If an OS/2 application consists of only one file with the .EXE extension and uses no secondary files, execute permission is sufficient. However, read (R) permission is required to run .BAT and .CMD files. To run DOS applications, users must have read permission.

Applications often use secondary files, such as help files or a dictionary file used by a text editor, and users need at least read permission for these files. Read permission lets users read, execute, and copy files. You can assign read permission to the alias containing the application’s secondary files, and then create a separate access control profile for the first executable (.EXE) file with execute permission only. This restriction prevents users from copying the primary executable file.

If an application creates a temporary file, both create (C) and read (R) permissions are required. If a user needs to edit the temporary file, write (W) permission is also necessary.

Directory resources with write permission also need attributes (A) permission if they are used in applications that change file attributes. For example, if a directory resource does not have attributes permission and an attempt to write to the file changes file attributes such as date and time, the attempt fails.

Defining the Application

Define the application as a public OS/2, DOS, or Windows application through the Public Application Definitions notebook of LAN Server Administration. Steps for defining a public application are in “Defining Public Applications” on page 118.

You, as a system administrator, can define your own private OS/2 applications. Network users can also define and manage their own private applications, which can be located either on their workstation or on a server.

Some benefits of defining a public application are:

- The application uses disk space only on the server instead of on every workstation.
- Users can directly access applications without having any knowledge of the network configuration.
- Setting up and maintaining the necessary configuration of network resources required by the application is easier.
- Running applications from program starters (either the Network Applications folder, the Run Applications window, or the **LAN Applications** list in the Application Installation window) is easier than running them from the command line.

The definition of a network application enables the system to locate and start the first executable file of the application. If the application uses additional files, make sure the first application file can run or read the other files as needed. For more information, refer to the publications that come with your application.

Note: You can assign DOS applications to users at OS/2 clients. You can also set up DOS applications to run as OS/2 public or private applications.

Customizing Applications

When you customize an application, you make changes in the steps for setting up an application to meet your needs or the needs of your users. Consider the following when customizing an application:

- You can create multiple application definitions, each using different network resources. You can model new application definitions on existing ones.
- The application can require you to set environment variables in a batch file before running the application.
- The application can collect parameters (for example, *printername* or *username*) at run time for use in conditional batch processing. Use the IF and GOTO batch commands for this purpose. Refer to the *Command Reference* for more information about command descriptions.

  For example, if the application uses a printer and a default printer of LPT1 is specified, you can allow use of alternate printers by putting a check mark in the **Prompt for additional parameters** field when defining the application. Different printer names can be handled by combining IF, GOTO, and NET USE commands in a batch file that subsequently starts the desired application.
- To alter an application for a specific user, prepare a batch file that calls a secondary batch file containing commands the user needs. (The secondary file can be located on a server, for example, in the user's home directory, so that you can manage it.) If the secondary batch file is found, it performs the desired setup and program call. If it is not found, the application proceeds normally.

  For example, an application batch file can test for the existence of a secondary batch file in the user's home directory, containing a NET USE command to a specified plotter. If found, this secondary batch file runs, giving the application access to the plotter in addition to the network assignments defined for the application.

Managing Network Applications

This section contains procedures for managing the public applications of users on the network and managing your own private applications. You can add, delete, and update public applications for specific users or for all the users defined in a group.

For more information, see:

- “Public Applications” on page 118
  - “Defining Public Applications” on page 118
  - “Adding Public Applications for Users” on page 119
- “Private Applications” on page 119
  - “Defining Private Applications” on page 119
  - “Updating Private Application Definitions” on page 120
  - “Deleting Private Application Definitions” on page 120

Public Applications

The system administrator sets up public applications for users at WorkSpace On-Demand, OS/2, and DOS clients. You can define WorkSpace On-Demand, OS/2, DOS, and Windows public applications to the network and add them to users' program starters. You can also update and delete definitions for public applications.

When a user at a WorkSpace On-Demand client logs on, any publications assigned to them are placed on the desktop.

When a user at an OS/2 client logs on, any public applications assigned to the user are included in the Network Applications folder.

When a user at a DOS LAN Services client without Windows logs on, the system updates the Run Applications window with the DOS applications you set up as public applications.

DOS LAN Services users with Windows can view DOS public applications as shared applications. When a user at a DOS LAN Services client with Windows logs on, the system lists shared applications in the user's **LAN Applications** list, which is in the Application Installation window.

Only administrators and users with Server operator privilege can set up public applications. However, both users and administrators can determine which public applications display on the program starter.

For more information, see the following topics:

- "Defining Public Applications"
- "Adding Public Applications for Users" on page 119

Defining Public Applications

Use the next procedure to define public WorkSpace On-Demand, OS/2, DOS, or Windows applications.

To define WorkSpace On-Demand, OS/2, DOS, and Windows applications as public applications:

1. Open **LAN Server Administration**.
2. Open the domain object in which you want to create public application definitions.
3. Open **Public Application Definitions**.

   The Public Application Definitions folder is displayed.
4. To create a new definition, drag a copy of the **WorkSpace On-Demand Template**, **OS/2 Template**, or **DOS & Windows Template** to an open area of the folder.
5. Complete the fields on the pages under each tab. Required fields are identified by an asterisk (*).
6. After you complete and check the pages, select **Create**.

Note: You can customize WorkSpace On-Demand applications through the use of application parameters. For more information on this, refer to the *WorkSpace On-Demand 2.0 Administrator's Guide*.

Adding Public Applications for Users

Adding applications to users' program starters makes the applications convenient.

To make WorkSpace On-Demand, OS/2, DOS, and Windows public applications easily available to users:

1. Open **LAN Server Administration**.
2. Open the domain object.
3. Open **Public Application Definitions**.
4. Open either **User Accounts** or **Groups**.
5. Drag the appropriate application object from the **Public Application Definitions** folder and drop the object on the appropriate user or group.

   The Add Public Applications window is displayed.
6. Select **OK**.

Private Applications

Users at OS/2 clients can create private OS/2 applications through LAN Server Administration. The network administrator must, however, first set up aliases and access control profiles for the resources before the user can use the application. Then when a user at an OS/2 client logs on, the private applications are automatically added to the Network Applications folder.

Refer to the *DLS and Windows User's Guide* for information on setting up private DOS applications for DOS LAN Services users.

DBCS Note: You do not have the online reference on DOS.

You can define private applications to the network. You can also update and delete definitions for private applications.

For more information, see the following topics:

- "Defining Private Applications"
- "Updating Private Application Definitions" on page 120
- "Deleting Private Application Definitions" on page 120

Defining Private Applications

Use the next procedure to create the definition for a private application.

To define a private application:

1. Open **LAN Server Administration**.
2. Open the domain object in which you want to create private application definitions.
3. Open **User Accounts**.

   The User Accounts folder is displayed.
4. With mouse button 2, select a user account object.
5. From the pop-up menu, select the arrow to the right of **Open as**.
6. Select **Private applications**.

   The Private Applications Definitions folder is displayed.

7. To create a new definition, drag a copy of the **OS/2 Template** to an open area in the folder.

   The Private Applications notebook is displayed.
8. Complete the fields on the pages under each tab. Required fields are identified with an asterisk (*).
9. After you complete and check the pages, select **Create**.

You can run the application from the program starter after you log off and on.

Updating Private Application Definitions

Use the next procedure to change the definition for a private application.

To change private application definitions:

1. Open **LAN Server Administration**.
2. Open the domain object.
3. Open **User Accounts**.

   The User Accounts folder is displayed.
4. With mouse button 2, select the user account you want to work with.
5. From the pop-up menu, select the arrow to the right of **Open as**.
6. Select **Private applications**.

   The Private Applications Definitions folder is displayed.
7. Open the private application object for which you want to update the definitions.

   The notebook of the selected application is displayed.
8. Select the tabs for the pages you want to update.
9. Update the properties.
10. Select **Set**.

Deleting Private Application Definitions

Use the next procedure to remove the definition for a private application.

To delete a private application definition:

1. Open **LAN Server Administration**.
2. Open the domain object.
3. Open **User Accounts**.

   The User Accounts folder is displayed.
4. With mouse button 2, select the user account for which you want to delete a private application definition.
5. From the pop-up menu, select the arrow to the right of **Open as**.
6. Select **Private applications**.

   The Private Applications Definitions folder is displayed.
7. With mouse button 2, select the private application for which you want to delete the definition.
8. From the pop-up menu, select **Delete**.
9. Select **Delete** in the confirmation window.

OS/2 Applications Using Dynamic Link Libraries

The OS/2 dynamic link library (DLL) feature allows multiple applications to call common modules.

The LIBPATH statement in the CONFIG.SYS file must specify the location of DLL files. If any application files end with the .DLL extension, you must edit the CONFIG.SYS file of each workstation where the application runs to indicate where DLL files are for that application. Because the OS/2 program supports UNC names, you can specify a server name and netname in the LIBPATH statement. For changes to the LIBPATH statement to become effective, you must shut down the operating system from the desktop, and then restart the workstation by pressing Ctrl+Alt+Del. The LIBPATH statement is unlike the SET PATH statement, which does not require starting the workstation again for changes to become effective.

For more information, see the following topics:

- “Creating a Subdirectory for DLL Files”
- “Specifying the Location of DLL Files”

Creating a Subdirectory for DLL Files

If more than one application uses DLL files, keep all DLL files (for all applications) in a separate subdirectory on the server. Then specify the path to the subdirectory in the LIBPATH statement on each workstation.

If DLL files are on several servers, add a UNC name containing each server name and subdirectory to the CONFIG.SYS file LIBPATH statement for a user to access those applications.

To create and prepare a subdirectory for DLL files:

1. Create a subdirectory on the server drive C for the DLL files, such as \DLLIB on SERVER1.
2. Create an alias for the subdirectory, such as DLL. Share this alias at server startup to allow access to these DLL files at all times.
3. Create an access control profile for the alias, allowing users using applications with DLL files to have read permission.
4. Edit the CONFIG.SYS file on each client to add the server name and the netname (the netname value is the same as the alias). The following example uses values from the previous steps:

   ```
   \\SERVER1\DLL
   ```

Specifying the Location of DLL Files

You can also specify the location of DLL files by keeping all the application files, including the DLL files, in the same subdirectory or you can define a working directory where the DLL files are located. Following are general steps to perform these actions:

- Put all of the application files, including DLL files, in the same subdirectory and perform the following steps:
  1. When you define the application, define a working directory with an assigned drive, for example, drive T.

2. Edit the CONFIG.SYS file on each client to add the working directory drive to the end of the LIBPATH statement. In this example, add the following:

   ```
   T:\;
   ```

   To avoid conflicts among users on the client, tell your users not to make resource assignments to this drive.

- Define a working (current) directory for the application where the DLL files are located. In the LIBPATH statement, append a period followed by a semicolon (;) to tell the OS/2 program to search the current directory for DLL files. When the application is run, the OS/2 program searches the working directory for the DLL files. If this method is used, users must not change the current directory while using the application.

Stopping Applications at Logoff

When you log off from a server, OS/2 Warp Server or LAN Server prompts you if an application is still running. At the prompt you can either cancel the logoff or stop the application.

If you want to stop any network application at logoff without being prompted, type the /Y parameter as follows:

```
LOGOFF /Y
```

Note: If you log off while OS/2 network applications are accessing DLLs from the server, those applications will trap. In most cases, the trap will not affect the operation of other software (including the OS/2 operating system) on the client. To avoid traps, always close your network applications before logging off.

Defining Network Messaging as a Public Application for DOS LAN Requester 3.0 Users

If you have DOS LAN Requester 3.0 users who are not upgrading to DOS LAN Services, the DOS LAN Requester Messaging program does not display on their Served Applications program starters after the server is upgraded to LAN Server 4.0 or OS/2 Warp Server.

DOS LAN Services provides a new Network Messaging GUI; however DOS LAN Requester 3.0 users are unable to access it because the DOS LAN Requester interface is incompatible.

In order to provide DOS LAN Requester users with a messaging service, you can define the messaging service used in DOS LAN Requester 3.0 as a public application. You must create an alias for the application and define an access control profile for the alias before adding the program to users' Served Application groups.

To create an alias and access control profile for the messaging program:

1. Copy the following files from the\DOSLAN directory on a DOS LAN Requester 3.0 workstation and place them in the OS/2 Warp Server or LAN Server \IBMLAN\DOSLAN\NET directory:
   - DMPC.EXE
   - CMM_MAIN.EXE

- CEIM.CNF

2. At the server, open **LAN Server Administration**.
3. Open the domain you want to access.
4. Open **Directory Resource Definitions**.
5. Drag and drop the **Directory Template** to an open area in the folder. The Identity page of the notebook is displayed.
6. Complete the Identity page as follows.
   - **Alias:** DLRMSG
   - **Description:** DLR Messaging Program
   - **Server:** (name of server where program resides)
   - **Path:** C:\IBMLAN\DOSLAN\NET
   - **When shared:** At server startup
   - **Maximum connections:** Unlimited
7. Select **Create**.
   - If there is no access control profile, a message is displayed prompting you to create one. Select **OK** to create the access profile.

     The Identity page of the Access Control Profile - Create notebook is displayed.
   - If there is an access control profile, no message appears. The Identity page of the Access Control Profile notebook is displayed.

   See “Chapter 7. Defining Access Control Profiles” on page 83 for information about access control profiles.
8. Select the **Permissions** tab.
   - **If the user is listed:**
     a. Select the user IDs from the list on the left.
     b. Select **Replace**.
     c. Select Read (**R**) and Execute (**X**) permissions from the list on the right.
     d. Select **Change**.

        The permissions you selected appear beside the user IDs in the list on the left.
   - **If a user is not listed:**
     a. Select **Add**.

        The Add Access Control Entries window is displayed.
     b. Select the user ID from the list on the left.
     c. Select Read (**R**) and Execute (**X**) permissions from the list on the right.
     d. Select **OK**.

        The user ID appears on the Permissions page with Read (**R**) and Execute (**X**) permissions.
9. Select **Create** or **Set**.

   A message is displayed prompting you whether to propagate the access permissions to all subdirectories in the path. See “Propagating Access Control Profiles to Subdirectories” on page 88 for information about propagating (applying) an access profile to subdirectories.
10. Select **OK** to propagate access to all the subdirectories in the path, giving users Read (**R**) and Execute (**X**) access to the entire program directory tree.

The alias DLRMSG is created, the directory is shared, and the access control profile is created. An icon representing the alias is added to the Directory Resource Definitions folder in the domain.

To define the program as a public DOS application using the alias:

1. Open **LAN Server Administration**.
2. Open the domain you want to access.
3. Open **Public Application Definitions**.
4. Drag and drop the **DOS & Windows Template** to an open space in the folder. The Public Application Definition notebook is displayed.
5. Complete the Identity page as follows:
   - **Application name:** DLRMSG
   - **Description:** DOS LAN Requester Messaging
6. Select the **Invocation** tab and complete the fields as follows:
   - **Command:** DMPC
   - **Parameter:** %XSLCNF% CMM_MAIN.EXE
   - **Prompt for additional parameters:** (Do not check)
7. Select the **Program Location** tab and complete the fields as follows:
   - **Alias:** DLRMSG
   - **Remaining path to program:** (Accept default)
   - **Assigned drive:** Next available (Accept default)
8. Select the **Work Directory** tab and complete the fields.
   - **Alias:** DLRMSG
   - **Remaining path to program:** (Accept default)
   - **Assigned drive:** Next available (Accept default)
9. Select **Create**.

   The public application is created and an icon representing the DOS public application definition for the DOS LAN Requester Messaging program is added to the Public Application Definitions folder in the domain.

In the next series of steps you will add the DOS LAN Requester Messaging program to a user’s program starter.

To add the DOS LAN Requester Messaging program to a user’s program starter:

1. Open **LAN Server Administration**.
2. Open the domain you want to access.
3. Open **User Accounts**.
4. Open the user account to which you are adding the DOS LAN Requester Messaging program.

   The notebook of the selected user account is displayed.
5. Select the **Applications** tab.
6. Select **Add** to display the Add Public Applications window.
7. Select **DLRMSG** and then select **Add**.

   The DOS LAN Requester Messaging program is added to the user’s program starter as a public application.
8. Select **Set** to save changes to the user account properties and close the notebook.

If the user account is logged on, the user must log off and then log on again before using the application. This step adds the application to the user's program starter.

Preparing to Run Programs Remotely

You usually run programs remotely by entering the NET RUN command at the command line interface. You can also use the AT and NET ADMIN commands. For more information about command descriptions, refer to the *Command Reference* . For information on running a program, refer to the *OS/2 File and Print Client Guide*.

Consider the following methods and constraints when preparing to run programs remotely.

- To find out if a program can be run remotely, type the following command at the command prompt on the server:

  ```
  DETACH command <NULL> outfile 2>&1
  ```

  where *command* is the program to run and *outfile* is the name of the file that contains output. To display the output of *command*, type `TYPE outfile`. Examine the information in *outfile* to make sure the expected results were obtained. Information in *outfile* contains standard output or error messages generated by running the program.

  Guidelines for developing a program to be run remotely are:

  - The program must have an .EXE extension.
  - The program must be a noninteractive, nonvideo mode program using standard input, output, and error file handles. The program must allow redirecting of these standard files.
  - The program must be able to be run in the background; that is, it must be able to do batch (instead of online) processing. You should be able to use the DETACH command on the program, as in the preceding example.

  The purpose of running a program remotely is to use the server's, rather than the client's, resources to run a program. Besides using the server's resources, the program to be run remotely does not inherit any environment. If you run a compiler, for example, environment variables you have set in the server, such as BIN and INCLUDE, are not valid with NET RUN.

- You must do the following to run a program on a remote server:
  - Access a server with the Netrun service started.
  - Be sure the **runpath** parameter in the Netrun section of the IBMLAN.INI file specifies the path to the .EXE program file. All other files must be in the working (current) directory. For more information, refer to *Performance Tuning*.
  - Determine commands you can run on the server, and identify the search path for these commands.
  - Assign a network drive to use as your current drive.
- All files used as parameters must be relative to the server, not to your workstation.

Be careful when granting access permissions to users for the RUNPATH directory. If you allow users *create* permission to files in the RUNPATH directory, they will be able to install and run programs that normally require administrator privilege. This is possible because the program is running on the server workstation and local API calls are not checked for authority level unless Local Security is running.

Chapter 10. Managing Windows Applications for DOS LAN Services

DOS LAN Services Windows allows users of Microsoft Windows 3.1 to access network files, printers, applications, and other services available on a OS/2 Warp Server or LAN Server domain through the Windows interface.

See the *DLS and Windows User's Guide* for information on DOS LAN Services Windows tasks such as logging on and off, using shared file resources and network printers, and sending messages.

This chapter describes how to set up DOS LAN Services Windows shared applications on the server, run them from the client, and give user groups access to the applications. This chapter also contains information on application configuration environment variables, DOS LAN Services Windows dynamic link libraries (DLLs), and the DOS LAN Services Windows message pop-up facility.

For more information, see the following topics:

- "Configuring for DOS LAN Services Windows Shared Applications"
- "Application Configuration Environment Variables" on page 128
- "WLRENV Environment Variable" on page 128
- "WLRWORKDIR Environment Variable" on page 129
- "DOS LAN Services Support Files for Windows" on page 130

Configuring for DOS LAN Services Windows Shared Applications

Use the following procedures to set up DOS LAN Services Windows shared applications.

To set up DOS LAN Services Windows shared applications:

At the server:

1. Install the application. Many Windows applications require installation through the Windows interface (available through a WIN-OS/2 command prompt).
2. Create a files alias for the directory containing the application. Create additional aliases for any other network resources required by the application. See "Using an Alias to Share a Resource" on page 70.
3. Assign access permissions for the aliases. See "Creating an Access Control Profile" on page 90.
4. Define both DOS and Windows applications as DOS public applications. See "Managing Network Applications" on page 117.
5. At the client, specify environment variables as needed. See "Application Configuration Environment Variables" on page 128.
6. Specify network assignments to be made when the application starts (optional).
7. Customize the application to meet your needs or the needs of your users.

At the DLS client running with Windows:

1. From the Program Manager window, open the **DOS LAN Services** program group.
2. Open the **DOS LAN Services** icon.
3. Select **Applications** from the menu bar.
4. Select **Shared Applications**. If **Shared Applications** is not selectable, you must log on to the domain where applications are available; then repeat this procedure from step 1.

   After selecting **Shared Applications**, the OS/2 Warp Server or LAN Server Application Installation window is displayed, containing two lists and four selections below the lists. The list on the left shows the LAN applications. The list on the right shows the user groups.

   To run a LAN application, first select the desired application, then select **Run**.

   To add a shared LAN application to a user group, first select the application and user group, then select **Add**.

   To create a user group, select **Create**, complete the **Description** and **Group File** fields, then select **OK**.

After a LAN application is installed into a Windows user group, you can either move or copy the application into otherWindows user groups. You can start the LAN application by opening its program icon.

Application Configuration Environment Variables

Certain applications manipulate resources and store data in ways that require you to alter the network environment to accommodate them. Generally, these applications require one or both of the following:

- More environment space than the default
- Their own working directories

For more information, see the following topics:

- “WLRENV Environment Variable”
- “WLRWORKDIR Environment Variable” on page 129

WLRENV Environment Variable

You can adjust the DOS Windows environment space by changing the WLRENV variable, which is 2048 bytes by default. Applications can require more or less than this amount. If you need to adjust the environment space, you must change the WLRENV variable before starting Windows.

The format of the environment variable is:

```
SET WLRENV=nnnn
```

where *nnnn* equals any value allowed by DOS.

Use these steps to double the environment space for a Windows session:

1. At the DOS prompt, type `SET WLRENV=4096` and press Enter.
2. Start Windows by typing `WIN` and pressing Enter.

WLRWORKDIR Environment Variable

You can establish a working directory for a shared application that requires one. DOS LAN Services Windows working directories can be set with a local environment variable at a workstation to allow the user to override the one defined by the administrator.

Note: This environment variable overrides any working directory assignment associated with the shared application. It is not required.

If the WLRWORKDIR environment variable is set to some nonempty string, the value of this environment variable sets the working directory. For example, if you enter the DOS command `SET WLRWORKDIR=C:\HOME`, the system sets the current directory to C:\HOME.

The format of the WLRWORKDIR variable is:

```
WLRWORKDIR=d:\symbol
```

where *d* is either defined as the logical drive or specified with the *%w* symbol. The following predefined symbols increase the flexibility of this variable. If any of these predefined symbols are present in the WLRWORKDIR string, they are replaced with other characters before the working directory is set. If no drive letter or drive letter variable is specified, the default is the current drive.

The following list shows predefined symbols.

Symbol	Substitution
%w	Drive letter for the application working directory (as defined at the server and connected at program startup)
%p	Drive letter for the application program directory (as defined at the server and connected at program startup)
%a	Application's program alias
%u	Logged-on user's user ID
%d	Logged-on user's OS/2 Warp Server or LAN Server domain
%%	%

The following example sets the working directory at program startup to C:\ *userid*\ *program-alias*:

```
WLRWORKDIR=C:\%u\%a
```

This example would support a convention where users have a user name directory at their workstations with a program-specific subdirectory below it.

The following example sets the working directory at program startup to the program working directory (as defined at the server) plus a user-specific subdirectory named the same as the logged-on user ID:

```
WLRWORKDIR=%w:\%u
```

Notes:

1. The case of the predefined symbols is significant; you must type them in lowercase for substitution to occur.

2. Predefined symbols and characters to be interpreted can be combined in whatever order is useful for your installation, as long as the resulting string, after substitution, defines a valid path. If a drive letter is not given as part of the expanded WLRWORKDIR value, the string is interpreted as a subdirectory below the current directory, the same as though a change directory (CD) command were issued from DOS.
3. After a substitution of special symbols, the specified working directory must exist on the specified drive or below the current directory if no drive is specified. The directory is not created automatically when starting the application. If the given directory does not exist, the working directory is not set properly.

   This method of setting the working directory is not supported by the non-Windows version of DOS LAN Services.

DOS LAN Services Support Files for Windows

The following sections describe the DOS LAN Services Windows interface and the Windows message pop-up facility.

For more information, see the following topics:

- “Windows Network Interface”Windows Network Interface
- “Message Pop-Up Facility” Message Pop-Up Facility

Windows Network Interface

In Windows, DOS LAN Services requires the following data link library files (DLLs) to perform network tasks such as displaying active servers, browsing available resources, and managing printer queues:

- NETAPI.DLL
- PMSPL.DLL

The following files provide the connection betweenDOS LAN Services and Windows:

- WINDLS.DLL
- DLSNET.EXE
- RUNLSAPP.EXE
- DLSNET.DRV

The files in both lists, plus the DLSNET.HLP and WINPOPUP.EXE files, are provided on the DOS LAN Services diskettes and are installed with DOS LAN Services.

If your application uses DLL files, you can specify a working directory.

Message Pop-Up Facility

The message pop-up facility for Windows is WINPOPUP.EXE. The WINPOPUP.EXE file works in conjunction with the NET START command. The messaging pop-up is loaded into memory with the NET START NETPOPUP command or with the NET START command if NETPOPUP is on the autostart line of the NETWORK.INI file. The WINPOPUP.EXE file displays received messages while the Windows GUI is active.

Chapter 11. Network Printing

Network printers are managed through individual *printer objects* (objects that represent a physical printer, its printer driver, queue, and other settings). By default, printer objects are created as printer queues. You can manage printer objects on remote servers, from any client, by accessing the printer object from the Network folder.

An administrator, or a user with Print operator privilege, can manage any print job, printer queue, or printer object. Users can hold, release, and cancel their own print jobs. You can also allow a user to manage network printing.

This chapter provides some examples of how to install a printer at a server and how to manage network printers using OS/2 Warp Server or LAN Server. For more information about printer objects and the Network folder, see the *OS/2 Desktop Guide* .

For more information, see the following topics:

- "How to Grant Print Operator Privileges to a User"
- "Printing from a Client" on page 132
- "Installing a Network Printer at a Server" on page 133
- "Managing Network Printers" on page 134
- "Example: Setting Up a Printer Object for a 4019 Printer at the Server" on page 136
- "Example: Creating a Network Printer Object for an OS/2 Client" on page 139

How to Grant Print Operator Privileges to a User

A user with operator privileges has certain administrative capabilities but is not a full administrator. A user may have one or more operator privileges, including the Print operator privilege. The Print operator privilege permits a user to manage printer queues and print jobs remotely. The user can, either from the command line or from a Print object, create, modify, and delete printers and queues. The user can also share printer queues and manage remote jobs on shared queues.

Operator privileges are part of the accounts database and are replicated within a domain. The following procedure shows how to grant a user Print operator privilege through the OS/2 Warp Server Administration.

To grant or revoke Print operator privilege for a user:

1. Open **OS/2 Warp Server Administration**.
2. Open the domain object.
3. Open **User Accounts**.

   The User Accounts folder is displayed.
4. Open the user account for which you want to change privileges.

   The first properties page is displayed.
5. Select the **Privileges** tab.

   The Privilege page is displayed:

6. Select **User**.

   This choice denies administrator permissions to the user.
7. Select **Print – Manage printer queues** in the **Special Privileges** list to grant Print operator privilege.

   Deselect the check box to revoke the privilege.
8. Select **Set** or **Apply**.

A system administrator can also use the NET USER command to grant or revoke Print operator privileges to users. For example, to give the Print operator privilege to a user, type:

```
NET USER userid /OPERATOR:PRINT
```

Note: In the previous example, the NET USER command runs at either the domain controller or in combination with the NET ADMIN command directed to the domain controller.

See the *Command Reference* for more information about the NET USER command and operator privileges.

Printing from a Client

When you submit a print request on the network, your print job is added to the queue belonging to the printer object or port you selected, and the data is stored on the server's hard disk until the job has been printed. OS/2 Warp Server and LAN Server support various types of printing. You can print from the desktop using direct manipulation. You can print outside the desktop using OS/2 and NET commands, or you can print from an application.

Printer objects, which are operating system components, allow you to see all the print jobs for selected queues and hold, release, or cancel any job you submitted. You can access remote printer objects through the Network folder. See the *OS/2 Desktop Guide* for more information about printing from the desktop and managing your print jobs.

Note: When printing from a LAN Requester to a network printer, both the LAN Requester and server must have the same level printer driver.

For more information, see the following topics:

- “Printing Using OS/2 and NET Commands”
- “Printing from a Presentation Manager Application” on page 133

Printing Using OS/2 and NET Commands

You can print text files using the OS/2 COPY command or the NET COPY command. If you want to send a print job across the LAN, then you only need to use a shared printer object. No other setup is required.

The following example shows how to use the OS/2 COPY command to print a file named REPORT.TXT on the printer associated with the printer port LPT3. Connect to the printer by assigning LPT3 to the network printer with the NET USE command. For example, to connect to the printer named PR3812 on the server named DEPT452, you would type:

```
NET USE LPT3 \\DEPT452\PR3812
```

To print the file from LPT3, type:

```
COPY REPORT.TXT LPT3
```

The following example shows how to use the NET COPY command to print a file named REPORT.TXT on the printer associated with the shared printer object PRINTQ on the server LASER1:

```
NET COPY REPORT.TXT \\LASER1\PRINTQ
```

Printing from a Presentation Manager Application

Printing from a Presentation Manager application requires that you select a printer object name instead of a port. The Enhanced Editor is an example of an application that requires you to select a printer object name.

For information about setting up to print on a network printer from a Presentation Manager application, see the *OS/2 Desktop Guide*.

Installing a Network Printer at a Server

Network printing uses the printer object functions of the operating system as well as of OS/2 Warp Server or LAN Server. Complete the following tasks to install a network printer.

To install a network printer at the server:

1. Attach the printer to the print server. Refer to the documentation that came with your printer for more information.
2. Create a printer object. See “Creating a Printer Object” on page 136 for more information.

   If necessary, install a printer driver that matches the attached printer. See “Installing a Printer Driver” on page 136 for more information.
3. From the printer object, change the print properties as needed.
4. From the graphical user interface, share the printer object. See “Creating a Printer Alias” on page 137 for information about creating the alias and giving users appropriate access.

For more information, see the following topic:

- “Installing and Configuring Network Printers for DLS Windows”Installing and Configuring Network Printers for DLS Windows

Installing and Configuring Network Printers for DLS Windows

To use a network printer from DOS LAN Services running on Microsoft Windows, you must install the appropriate printer driver on each workstation. To do so, follow these steps:

To install a network printer at a DLS Windows workstation:

1. Select **Control Panel** from the Program Manager window.
2. Select **Printers**.
3. Select **Add Printer**.
4. Select the printer driver for the network printer you want to use from the **List of Printers** list.

5. Select **Install**.

   If the driver already exists, select **Current** from the Printers–Configure window.

   If the driver does not exist, you are prompted to insert the appropriate Windows diskette.
6. Select **Configure** from the Printers window.
7. Select any port for the printer you are configuring, and then select **Setup**.

   Note: Even though DLS Windows requires that you specify a port here, your choice has no effect on how the network printer is connected.
8. Complete the information for the printer you have selected in the Printers window, and then select **OK**.
9. Select **OK**.
10. Select the new printer from the Printers–Configure window, and then select **Active** from the **Status** list.
11. To make the new printer the default printer, select it, and then select **OK** to exit the Printers window.

Managing Network Printers

You can send print jobs to printer objects according to general criteria, such as file size. For example, you can set up one printer object for large jobs and another printer object for small jobs. Each job waits in the queue associated with the printer object until the job prints on one of the printers that the printer object uses. You can define a printer object to use just one printer or, to make better use of available resources, to use several printers at once (called pooling printers). For information about pooling printers, see the *OS/2 Desktop Guide*.

You can specify several network options for printer objects that are shared on the network; for example, a separator page file queue start and stop time and the refresh interval.

You can hold or release a printer object. You can also hold, release, or cancel particular jobs within a printer object. You can remotely manage printer objects by accessing the printer object from the Network folder.

For more information, see the following topics:
- “Updating OS/2 Printer Object Settings”
- “Description of Printer Settings” on page 135

Updating OS/2 Printer Object Settings

Perform the following procedure to update printer settings. You can change the:
- Way in which the printer queue is displayed
- Frequency with which the display of the printer queue is refreshed
- File that contains the page that separates print jobs
- Time at which a print job must start or end

Refer to “Description of Printer Settings” on page 135 for a description of the settings.

To update printer settings:

1. Select the printer object you want to update. To make changes at a remote server, select the printer object from the Network folder.
2. Press mouse button 2 to display the pop-up menu for the printer object.
3. Select **Properties**.

   To specify network job view:

   a. Select the **View** tab.
   b. Select either **Show all jobs** or **Show own jobs**.

   To specify the refresh interval:

   a. Select the **View** tab.
   b. Specify a refresh interval in seconds.

   To specify the separator file:

   a. Select the **Print options** tab.
   b. Specify a separator file name.

   To specify the start time and stop time:

   a. Select the **Print options** tab.
   b. Specify a start time and stop time.

Description of Printer Settings

Following are the descriptions of some of the printer settings that can be set for remote printer objects. There are other settings not listed that are used to manage the local printer at the server. Refer to the *OS/2 Desktop Guide* for more information about changing these local printer settings.

Option **Description**

Network job view
Specifies whether all jobs or only jobs owned by the user are displayed in icon or detail view. This item is not available if the printer object is not remote.

Refresh interval
Sets the rate at which the printer object window is refreshed with the latest network jobs. The default rate is 45 seconds. Local jobs are updated as status changes occur.

Separator file Specifies a file name containing information about the separator page used for network print jobs. This separator page prints before each job. It can contain, for example, a user ID, a job number, and the time the job is printed.

Start time Specifies when the printer object starts printing jobs. Specify this option as a time in 24-hour *hh:mm* format. If the start time and stop time are the same, the printer object prints continuously.

Stop time Specifies when the printer object stops printing jobs. Specify this option as a time in 24-hour *hh:mm* format.

Example: Setting Up a Printer Object for a 4019 Printer at the Server

DBCS Note: The 4019 printer is not used on DBCS systems. However, you can use this example as a procedure for setting up a printer object for other printers used with your system.

Following are the tasks for installing a 4019 printer using a parallel (LPT) port.

For more information, see the following topics:

- “Creating a Printer Object”Creating a Printer Object
- “Installing a Printer Driver”Installing a Printer Driver
- “Creating a Printer Alias” on page 137Creating a Printer Alias

Creating a Printer Object

Use the next procedure to create an object for the printer.

To create a printer object:

1. Open the **Templates** folder on the desktop.
2. Select the **Printer** template, drag it to a folder or an available space on your desktop, and drop it.
3. Complete the Create a Printer window:

Field	**Value**
Name	LASER1
Default printer driver	(Accept the default)
Output port	LPT1

4. Select **Create** when you are finished.

Installing a Printer Driver

You must now associate the printer object with the printer driver that matches the printer attached to the server.

To install a printer driver:

1. Place your cursor on the **LASER1** printer object and press mouse button 2 to display the pop-up menu.
2. Select **Properties**.

   The first properties page is displayed.
3. Select the **Printer Driver** tab.

   DBCS Note: The following statement about the IBM 4019 LaserPrinter does not apply to DBCS systems.

   If the IBM 4019 LaserPrinter is already included in the list of printer drivers, select it and close the notebook. The printer driver is installed.

   If it is not included in the list, continue with the rest of this procedure to install the printer driver.

4. Press mouse button 2 to display the pop-up menu for a printer driver.
5. Select **Install**.

   A list of OS/2 printer drivers is displayed in the Install New Printer Driver window. Scroll through the list of printer drivers until you reach IBM 4019 LaserPrinter.

   DBCS Note: Scroll through the list of printers until you reach the printer you want to install. Substitute your printer for the IBM 4019 LaserPrinter.
6. Select the IBM 4019 printer driver and then select **Install**.
7. Follow the instructions on the next window and insert the requested printer driver diskettes and select **OK**.

   Note: If you are installing the drivers from a CD-ROM, type the path to the OS/2 printer drivers instead of inserting diskettes.
8. Select **OK** when you are notified that the printer driver has been installed successfully.
9. Select **Cancel** from the Install New Printer Driver window when you are finished installing printer drivers.

Creating a Printer Alias

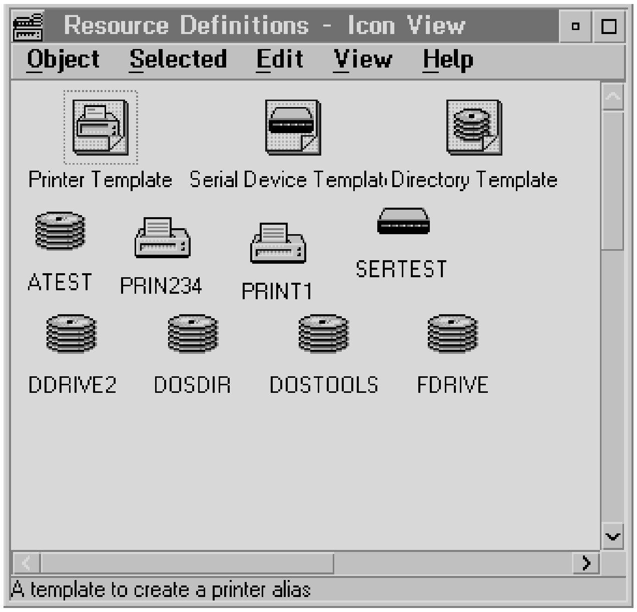
Printer aliases are nicknames for printer objects that are redirected to network printers. You can use aliases to represent shared printers, and you can create access control profiles for the aliases. Access control profiles specify what users or groups can access the printer.

Perform the following steps to create a printer alias. The server where the printer resides must be started and you must be logged on as an administrator.

To create an alias for a printer:

1. Open **LAN Server Administration**.
2. Open the domain object in which you want to create the alias.
3. Open **Resource Definitions**.

   The Resource Definitions folder is displayed.

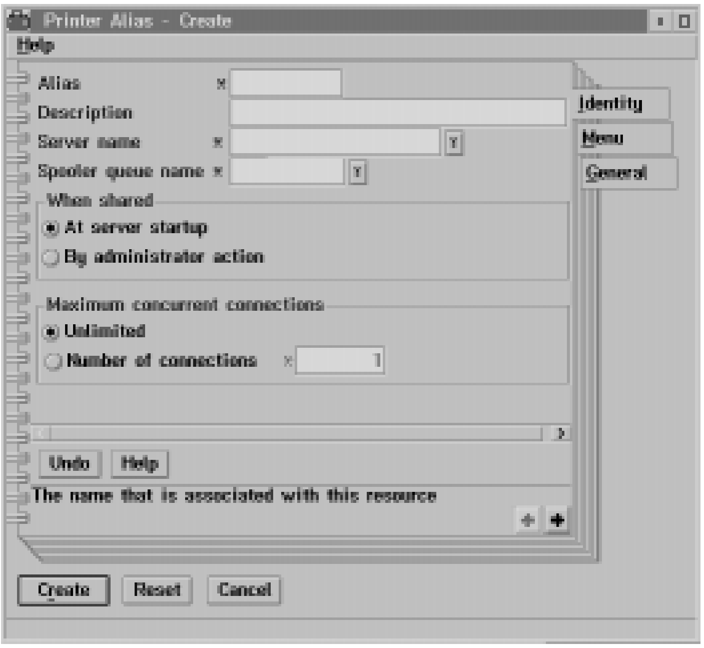


A template to create a printer alias

Figure 4. Resource Definitions Folder

4. Drag the **Printer Template** to a convenient location in the folder.

   The first properties page is displayed.



When shared
● At server startup
○ By administrator action

Maximum concurrent connections
● Unlimited
○ Number of connections 1

The name that is associated with this resource

Figure 5. Printer Alias Identity Page

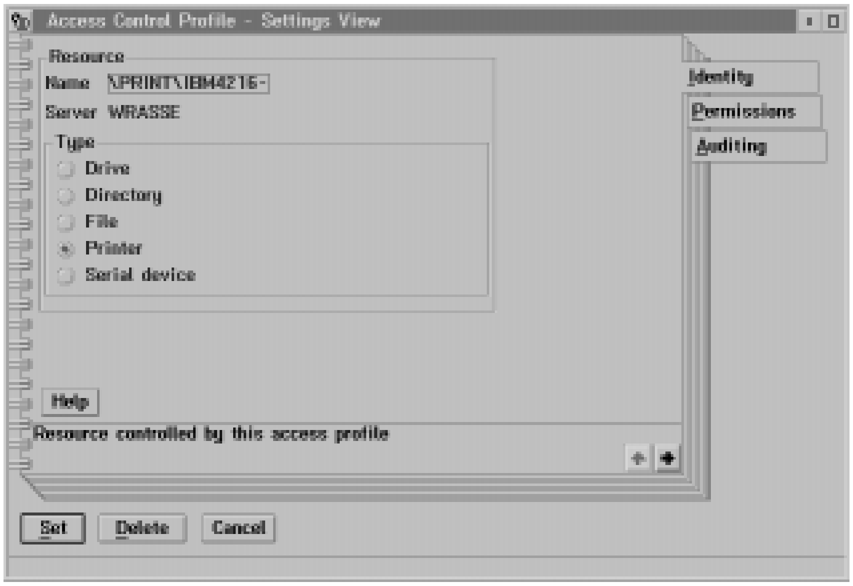
5. Type an alias name in the **Alias** field.
6. If you want, type a description in the **Description** field.
7. Select or type a server name:
   a. If the server where the resource is located is in this domain, select one of the server names in the **Server name** field.

   b. If the server where the resource is located is in another domain, type the name of that server in the **Server name** field.

8. Select or type a spooler queue name. The spooler queue name is the physical name of the printer queue which is displayed in the Properties notebook for the printer object.
9. Complete the Identity page.
10. Select **Create**.
    - If there is no access control profile, a message is displayed prompting you to create one. Select **OK** to create the access profile.

      The Identity page of the Access Control Profile notebook is displayed.
    - If there is an access profile, no message is displayed. The Identity page of the Access Control Profile notebook is displayed.

    See “Chapter 7. Defining Access Control Profiles” on page 83 for information about access control profiles.



Access Control Profile - Settings View

Resource

Name \PRINT\IBM4216-

Server WRASSE

Type

○ Drive

○ Directory

○ File

● Printer

○ Serial device

Resource controlled by this access profile

Figure 6. Access Control Profile Window

11. Complete the pages in the Access Control Profile notebook.

    Give the users and groups who need to use the printer Create (C) permission.
12. Select **Create** or **Set** to close the notebook.

Example: Creating a Network Printer Object for an OS/2 Client

The following example illustrates the steps required for an administrator and a user to set up a network printer object on an OS/2 client. The printer driver for the network printer needs to be installed on the OS/2 client workstation.

If the user does not have the correct printer driver installed, you can give the user the printer driver diskettes or share the directory where the printer drivers are contained on the server so they can be downloaded from the server.

The first part of the following example illustrates how to create the shared directory so users can download the printer drivers to their workstation. The second part illustrates how to add the network printer object to the user’s desktop.

To set up a shared directory for printer drivers:

The following steps are performed by the network administrator on the server. In our example, the 4019 network printer is attached to the server DONSRV.

1. Using LAN Server Administration, create an alias of 4019PRT for the network printer and create an access control profile to share the alias. Give users Create (C) access to the alias. See “Creating an Alias” on page 72 for steps on creating an alias and access control profile.
2. Create a directory named C:\DRIVERS on the server. Copy all the OS/2 printer driver files from the OS/2 printer driver diskettes or CD-ROM into the directory.
3. Create a directory alias named PRTDRIV for the C:\DRIVERS directory containing the printer drivers. Create an access control profile for the directory alias and give users Read (R) access.

Note: The printer drivers used by the server are actually stored in the C:\OS2\DLL\IBM4019 directory on the server DONSRV; however the alias PRTDRIV points to the directory named C:\DRIVERS which contains *copies* of the drivers.

To add the printer object to a user’s desktop:

The following steps are performed by the administrator or user at the OS/2 client.

1. Open the **Templates** folder on the desktop.
2. Drag and drop the **Network Printer** template onto an open area of the desktop.

   The Access Another Network Printer window is displayed.

   Note: You can also drag and drop the Network Printer template into the Network folder, where the network servers and aliases reside.
3. Complete the **Server** field by selecting the down arrow at the right of the **Printer** field to select a server or type the name of the server where the 4019 is attached. In this example, the server is named DONSRV.
4. In the **Resource** field, select the down arrow to select a queue name or type the queue name. In this example, you would select 4019PRT.
5. Select **OK**.
6. If a printer driver has not been installed, a window is displayed prompting you to install one. Select **Install**.
7. The next window prompts you to insert a diskette or type in the directory where the printer driver can be found.

   Because an alias (PRTDRIV) exists for a directory containing copies of printer drivers for a 4019 printer on the DONSRV server, type:

   ```
   \\DONSRV\PRTDRIV
   ```

   The printer drivers are installed on the OS/2 client and the Network Printer object is added to the user’s desktop.

Chapter 12. Managing the Network

Several OS/2 Warp Server or LAN Server functions allow you to manage the network effectively. You need not be at a server to complete most administrative tasks. You can complete most tasks, even those involving server changes, from any OS/2 LAN Requester on the domain.

For more information, see the following topics:

- "Managing Network Services"
- "Updating Parameters" on page 147
- "Viewing and Closing Open Files" on page 148
- "Viewing and Deleting Active Sessions" on page 149
- "Using Statistics" on page 149
- "Auditing" on page 151
- "Accessing Error Logs" on page 156
- "DOS and OS/2 Command Restrictions" on page 161
- "Managing More Than One Domain" on page 162
- "First Failure Support Technology/2 (FFST/2)" on page 162

Managing Network Services

Network services are programs that are part of OS/2 Warp Server or LAN Server. The available programs are identified in the\IBMLAN\IBMLAN.INI file. To control which services are started at startup, edit the IBMLAN.INI file on your workstation. Refer to *Performance Tuning* for more information.

Temporary changes to network services can be made through the OS/2 Warp Server Administration or the command line (instead of editing the IBMLAN.INI file).

Users can start and stop services available on their workstations. Some services can also be paused and continued.

The network services are briefly described in the following list. (For detailed descriptions of the services and information on their parameters, see *Performance Tuning*.)

Alerter
Notifies selected user IDs when problems occur. It also notifies the Generic Alerter service when certain LAN problems are detected or anticipated. This service cannot be paused.

DCDB Replicator
Copies the domain control database from a primary domain controller to one or more backup domain controllers.

Generic Alerter
Enables the server to build and send Systems Network Architecture (SNA) alerts. The Alerter service notifies the Generic Alerter service when certain LAN problems occur. This service cannot be paused.

LSserver
Provides DOS LAN Services support and logical server functions. The logical server supports remote requests from clients for

activities such as spooling, querying users, logon, and logoff. The default value for LSserver is to start when OS/2 Warp Server or LAN Server is installed. The user should never change the default. If you stop LSserver, the Server service automatically stops. Therefore, this service should never be stopped and cannot be paused.

Messenger Supports the receiving of messages at a client or server. This service cannot be paused.

NetLogon Copies the master user and group definitions file located on the domain controller to network servers. This service is available only on servers.

In order for the NetLogon service to replicate user and group definitions across servers in a domain, digit 3 of the **srvheuristics** parameter (on domain controllers) and digit 8 of the **wrkheuristics** parameter (on additional servers) must be left at their default values. If you change the defaults for these parameters, user and group data may not be replicated from the domain controller, resulting in unknown user IDs or group IDs on the additional servers. See “Domain User and Group Definitions” on page 44 for more information on using the NetLogon service.

Netrun Handles requests for running programs remotely on a server.

Network Neighborhood Browser Enabler
Allows OS/2 Warp Server to function as a master browser for Windows Clients. The master browser function provides Windows 95 and Windows NT clients the ability to view the domain’s LAN Server machines and their resources via the Network Neighborhood object.

Peer Allows one client to share resources with another. This service gives a client some of the capabilities of a server. You can administer a Peer server remotely. For information, see the *Command Reference*.

Remote IPL Allows the Server service to support remote initial program load (remote IPL) of workstations. This service corresponds to the Remoteboot section of the IBMLAN.INI file.

Replicator Copies files from a master location on a server to one or more servers or clients requiring a copy of the data. This service cannot be paused.

client Redirects requests for files, printers, and serial devices from one workstation to another workstation.

Server Receives and responds to network requests for files, printers, and serial devices. The service checks the requests against its database of user IDs and access permissions.

Timesource Designates a server as a source of a reliable time and date with which other workstations on the network can synchronize. The Timesource service does not keep time. It allows other workstations on the network to identify a server with a reliable clock. The default value for the Timesource service is to start on domain controllers when OS/2 Warp Server or LAN Server is installed. This service cannot be paused.

UPS Provides protection against power failure. If power is interrupted, the UPS service keeps the server running until the service can shut down the server safely or until an administrator stops the server.

For more information, see the following topics:

- “Network Service Status”
- “Starting a Network Service” on page 144
- “Stopping a Network Service” on page 145
- “Pausing a Network Service” on page 145
- “Continuing a Network Service” on page 146
- “Shutting Down the Domain Controller” on page 146

Network Service Status

The list below shows network service status types.

Status	Meaning
Started and active	The service is running normally.
Not started	The service has not been started.
Started and paused	The service has been stopped temporarily.
Started with pause pending	The service is about to pause.
Started with continue pending	The service is about to continue after being paused.
Stopping	The service is about to stop.
Starting	The service is about to start.

Through LAN Server Administration, you can manage network services and make temporary changes to the services’ parameters. Such changes remain in effect until the service is stopped or the value is overridden. You can change the state of services on your own workstation and on any server in the domain. However, to make parameter changes take effect each time the network software starts, you must edit the IBMLAN.INI file. For more information, refer to *Performance Tuning*.

For more information, see the following topic:

- “Guidelines for Stopping and Pausing Network Services”

Guidelines for Stopping and Pausing Network Services

Keep the following in mind when stopping and pausing network services:

- When the Messenger service is stopped on a workstation, that workstation can no longer receive messages or alerts.
- When the Requester service is stopped on a server, the server and OS/2 Warp Server or LAN Server program also stop. Users lose access to that server’s network resources. If any user is logged on at that server, stopping the Requester service logs them off. After the Server service stops on a server, that workstation can function only as a client and can no longer share resources with users.

- Pausing a client temporarily disables use of shared resources, but you are not disconnected from those resources. If you pause a server, no new requests to use the resources at that server are accepted. However, pausing a server does not affect files that are currently open or outstanding requests to use resources.

Pausing a network service can be used, for example, when preparing to shut down a server for maintenance. Before shutdown, you want to disallow further resource requests but allow current jobs in the server's spooler and serial device queues to complete processing until the queues are empty. Pausing the Server service disallows additional user connections to server resources, but allows current requests to complete processing.

Note: Administrators can connect to paused servers. This ability allows the server to be remotely administered.

You can disable user logon to a domain by pausing the NetLogon service on the domain controller and the other servers in the domain. This keeps new users from logging on. However, currently logged-on users and users with sessions to servers in the domain are not affected. To enable domain-validated logons again, continue the NetLogon service on the domain controller and the additional servers.

Starting a Network Service

Use the next procedure to start a network service.

To start a network service:

1. Open **LAN Server Administration**.
2. If the network service you want to open is on a remote server:
   a. Open the appropriate domain object.
   b. Open **Defined Servers**.
   c. Open the appropriate server object.
3. If the network service you want to open is on the local workstation, open **Local Workstation**.
4. Open **Services**.

   The details view of the Services folder is displayed so that you can view the current status of all installed services.
5. If you want to view more details of a particular service, double-click on its icon to display its notebook.
6. After you have viewed the properties, close the notebook.
7. With mouse button 2, select the service you want started.
8. From the pop-up menu, select **Start**.

   The Start Service window is displayed.
9. If you want to override the default parameters stored in the IBMLAN.INI file, change them in the **Parameters** field. If you leave the field blank, the default parameters are used.

   Changes you make here temporarily override the values in the IBMLAN.INI file. The changes remain in effect until you stop the service.
10. Select **Start**.

Note: You cannot start the Server service remotely.

Stopping a Network Service

Use the next procedure to stop a network service.

To stop a network service:

1. Open **LAN Server Administration**.
2. If the network service you want to stop is on a remote server:
   a. Open the appropriate domain object.
   b. Open **Defined Servers**.
   c. Open the appropriate server object.
3. If the network service you want to stop is on the local workstation, open **Local Workstation**.
4. Open **Services**.

   The details view of the Services Collection is displayed so that you can view the current status of all installed services.
5. If you want to view more details of a particular service, double-click on its icon to open its notebook.
6. After you have viewed the properties, close the notebook.
7. With mouse button 2, select the service you want stopped.
8. From the pop-up menu, select **Stop**.

Note: You cannot restart the Requester or Server service remotely. You cannot restart the Requester service from here.

Pausing a Network Service

Pausing a network service temporarily suspends the service. You can pause only the following network services:

- NetLogon
- Netrun
- Peer
- Requester
- Server

The Pause menu choice is not displayed for other services.

To pause a network service:

1. Open **LAN Server Administration**.
2. If the network service you want to pause is on a remote server:
   a. Open the appropriate domain object.
   b. Open **Defined Servers**.
   c. Open the appropriate server object.
3. If the network service you want to pause is on the local workstation, open **Local Workstation**.
4. Open **Services**.

   The details view of the Services Collection is displayed so that you can view the current status of all installed services.
5. If you want to view more details of a particular service, double-click on its icon to display its notebook.

6. After you have viewed the properties, close the notebook.
7. With mouse button 2, select the service you want paused.
8. From the pop-up menu, select **Pause**.

To resume a paused service, select **Continue**. See “Continuing a Network Service” for details.

Continuing a Network Service

Continuing a network service resumes the service’s functions after the service has been paused.

To continue a paused network service:

1. Open **LAN Server Administration**.
2. If the network service you want to continue is on a remote server:
   a. Open the appropriate domain object.
   b. Open **Defined Servers**.
   c. Open the appropriate server object.
3. If the network service you want to continue is on the local workstation, open **Local Workstation**.
4. Open **Services**.

   The details view of the Services Collection is displayed so that you can view the current status of all installed services.
5. If you want to view more details of a particular service, double-click on its icon to display its notebook.
6. After you have viewed the properties, close the notebook.
7. With mouse button 2, select the service you want continued.
8. From the pop-up menu, select **Continue**.

Shutting Down the Domain Controller

Shutting down the domain controller suspends all network services rendered to the users on the domain. It is important that the users be warned and given a chance to log off before the shutdown.

To shut down the domain controller:

1. Pause the NetLogon service:
   a. Open **LAN Server Administration**.
   b. Open the appropriate domain object.
   c. Open **Defined Servers**.
   d. Open the appropriate server object.
   e. Open **Services**.

      The details view of the Services Collection is displayed so that you can view the current status of all installed services.
   f. If you want to view more details of a particular service, open its icon. The notebook for that service is displayed.
   g. After you have viewed the properties, close the notebook.
   h. With mouse button 2, select **NetLogon**.
   i. From the pop-up menu, select **Pause**.

2. Broadcast a message to all users to log off:
   a. Open **Network Messaging**.

      The Network Messaging window is displayed.
   b. Select **Messages**.
   c. From the Messages pull-down menu, select **Send new**.
   d. In the message text field, type the message you want to send.
   e. Select **Broadcast** and follow the instructions in the window displayed.
   f. Select either a domain or the whole network and then select **OK**.
   g. Select **Cancel.** If you did not save your message, you are prompted to do so.

      View the list of logged-on users. Depending on your site's procedures, you may want to contact the remaining users individually.
3. Stop the Server service, and run Shutdown from the Desktop:
   a. Open **LAN Server Administration**.
   b. Open the appropriate domain object.
   c. Open **Object**.
   d. Select the arrow to the right of **Open as**.
   e. Open **Logged on users**.

      The Logged on Users window is displayed. It lists all the user currently logged on throughout this domain.
   f. After you have finished viewing this list, select **OK**.
   g. Notify any users still logged on to log off.
   h. Stop the Server service from LAN Server Administration.
   i. Run Shutdown from the Desktop to shut down the domain controller.

Updating Parameters

The definition parameters for servers and clients are stored in the IBMLAN.INI file for each workstation. To make permanent changes to these parameters, you must stop the Server or Requester service, edit the IBMLAN.INI file, and start the service again (refer to *Performance Tuning*). You can make temporary changes to a workstation definition without stopping the workstation and starting it again. These changes are in effect while the service is active.

For more information, see the following topics:

- “Updating Defined Server Parameters”
- “Updating Local Workstation Parameters” on page 148

Updating Defined Server Parameters

You can make temporary changes to a server's definition; for example, you can change the size of the audit file.

To make temporary changes to a server's parameters:

1. Open **LAN Server Administration**.
2. Open the appropriate domain object.
3. Open **Defined Servers**.
4. With mouse button 2, select the appropriate server object.

5. From the pop-up menu, select **Properties**.

   The server notebook is displayed. Server parameters are provided under the tabs.

6. Select each notebook tab successively, and change the appropriate parameters. For example, select the **Auditing** tab.

   The Auditing Page is displayed.

7. If you want to change the size of the audit file, type the new size in the Audit file size field. The default is 100KB.

   Changes you make here temporarily override the values in the IBMLAN.INI file. The changes remain in effect while the server is active. If you want to change the default parameters stored in the IBMLAN.INI file, change them in the parameters fields.

8. Select **Set**.

Updating Local Workstation Parameters

If your local workstation has LAN Requester installed, you can make temporary changes to its parameters with the following procedure.

To make temporary changes to a local workstation's parameters:

1. Open **LAN Server Administration**.
2. With mouse button 2, select **Local Workstation**.
3. From the pop-up menu, select **Properties**.

   The Local Workstation notebook is displayed. Workstation parameters are provided under the tabs.

4. Select each notebook tab successively, and change the appropriate parameters. For example, select the **Time-out** tab.

   Changes you make here temporarily override the values in the IBMLAN.INI file. The changes remain in effect while the client is active. If you want to change the default parameters stored in the IBMLAN.INI file, change them in the parameters fields.

5. Select **Set**.

Viewing and Closing Open Files

A file is *open* when its contents are being accessed. You can close an open file on a server to remove a deadlock situation between applications requiring the same file. You can also view and close files on a local workstation if it is a server.

To view and close open files on a server:

1. Open **LAN Server Administration**.
2. Open the appropriate domain object.
3. Open **Defined Servers**.
4. With mouse button 2, select the appropriate server object.
5. From the pop-up menu, select the arrow to the right of **Open as**.
6. Select **Open Files**.

   The Open Files window is displayed.

7. Select the file or files you want to close.
8. Select **Close File**.

9. Select **Close**.

Viewing and Deleting Active Sessions

A *session* is a logical connection between a server and a client. A connection begins when a request for a shared resource is successful. A OS/2 Warp Server or LAN Server client has only one session per server. In each session, however, a user can have multiple connections and open files. An additional server has an active session to the domain controller even when no user is logged on at the server. This session is listed in the display of active sessions. The **User ID** field is blank.

When a session is deleted, any files opened by the session are closed. A session is reestablished when the client contacts the server again for information or resource use.

You can also view and delete active sessions on a local workstation if it is a server.

To view and close active sessions on a server:

1. Open **LAN Server Administration**.
2. Open the appropriate domain object.
3. Open **Defined Servers**.
4. With mouse button 2, select the appropriate server object.
5. From the pop-up menu, select the arrow to the right of **Open as**.
6. Select **Active Sessions**.

   The Active Sessions window is displayed:
7. Select one or more active sessions to delete.
8. Select **Delete session**.
9. Select **Close**.

Using Statistics

The statistics function lets you see performance statistics for all of the servers on the domain. You can use the statistics to tune the performance of the network. Users can access statistics only for their own workstations. Additional statistics are available with the NET STATISTICS command. Refer to the *Command Reference* for more information.

For more information, see the following topics:

- “Viewing Statistics”
- “Printing Statistics” on page 150
- “Clearing Statistics” on page 150

Viewing Statistics

Use the next procedure to see the performance statistics for a remote server or local workstation. If the local workstation is not a server, only client statistics are available.

To view the statistics:

1. Open **LAN Server Administration**.
2. Open the appropriate domain object.
3. Open **Defined Servers**.
4. With mouse button 2, select the appropriate server object.
5. From the pop-up menu, select the arrow to the right of **Open as**.
6. Select the arrow to the right of **Statistics**.
7. Select either **Server** to view server statistics or **Requester** to view client statistics.

   The appropriate Statistics window is displayed.
8. When you have finished, select **Close**.

Printing Statistics

You can print the statistics on a network printer.

To print statistics on a network printer:

1. Open **LAN Server Administration**.
2. Open the appropriate domain object.
3. With mouse button 2, select the appropriate server object.
4. From the pop-up menu, select **Object**.
5. Select the arrow to the right of **Open as**.
6. Select the arrow to the right of **Statistics**.
7. Select either **Server** for server statistics or **Requester** for client statistics.

   The Statistics window is displayed.
8. Select **Print statistics**.

   Statistics for the selected server print at the default printer for that server.
9. Select **Close**.

Clearing Statistics

You can reset the values of all workstation statistics to 0. When you clear the statistics, the date and time statistics collection begins are set to the current date and time. Only an administrator can clear the statistics for a server. Users can clear the statistics only on their workstations. After you clear the statistics for a workstation, you cannot recover those values.

Use the next procedure to clear the statistics for a remote server or local workstation. If the local workstation is not a server, only client statistics are available.

To clear statistics:

1. Open **LAN Server Administration**.
2. Select the appropriate domain object.
3. Open **Defined Servers**.
4. Open the appropriate server object.
5. Select **Object**.
6. Select the arrow to the right of **Open as**.
7. Select the arrow to the right of **Statistics**.
8. Select either **Server** for server statistics or **Requester** for client statistics.

The appropriate Statistics window is displayed.

9. Select **Clear Statistics**.
10. Select **Close**.

Auditing

The OS/2 Warp Server or LAN Server *audit log* contains information about resource use and security. You can use audit log information for accounting, security, studying network use, or problem determination.

Each server keeps an audit log for the resources located on that server. The audit log can contain the following information. You can choose which of these resources to include in the audit log. You choose these resources by setting the **auditing** parameter in the IBMLAN.INI file or by specifying the /AUDITING parameter on the NET START command.

- Service state changes
- Successful and unsuccessful requests for session connection
- All requests for session connection
- Successful and unsuccessful requests for domain logon
- All requests for session connection and domain logon and logoff
- All logon and logoff requests (session and network)
- Successful and unsuccessful share requests
- All share requests
- Changes to user and group accounts database
- Changes to the access control database
- Resource access as defined by resource auditing options
- Logon limit violations

Additionally, you can specify that access attempts to a resource be recorded in the audit log when you create an access control profile for that resource. You can specify that all attempts, failed attempts, or no attempts to access the resource be recorded in the audit log.

For more information, see the following topics:

- “Checking the Status of Auditing”
- “Enabling Auditing and Audited Events” on page 152
- “Displaying the Audit Log” on page 153
- “Reversing the Order of Audit Log Entries” on page 153
- “Printing the Audit Log” on page 154
- “Writing the Audit Log to a File” on page 154
- “Clearing the Audit Log” on page 155
- “Changing the Size of the Audit Log” on page 155

Checking the Status of Auditing

Use the following procedure to determine whether auditing is enabled and which events are currently being audited.

To check the audit status:

1. Open **LAN Server Administration**.
2. Open the appropriate domain object.
3. Open **Defined Servers**.
4. With mouse button 2, select the appropriate server object.
5. From the pop-up menu, select **Properties**.

   The server notebook is displayed.
6. Select the **Auditing** tab.

   The Auditing page is displayed. It shows whether auditing is enabled, auditable events on the selected server, and which events are enabled for auditing.

   If the **Auditing enabled** check box is not active, the `Auditing` parameter in the IBMLAN.INI file is set to `No`.

   Note: You can change the audit file size on this page.
7. After you view the properties, select **Cancel** to close the notebook.

   Note: Use the **Cancel** button to prevent accidentally saving any unwanted changes you might have made while viewing the properties.
8. Select **Set** or **Apply**.

Enabling Auditing and Audited Events

If the **auditing** parameter is set to `NO` in the server IBMLAN.INI file, no auditing is done. You can choose which resources you want to include in the audit log by setting the **auditing** parameter in the server IBMLAN.INI file or by using the /AUDITING option on the NET START command.

To enable auditing of all events, type at the OS/2 command line:

```
NET START SERVER /AUDITING:YES
```

To keep only the logon, user list, and resource events in the audit log, type:

```
NET START SERVER /AUDITING:LOGON;USERLIST;RESOURCE
```

To keep all events except service events in the audit log, type:

```
NET START SERVER /AUDITING:YES /NOAUDITING:SERVICE
```

For more information on using the NET START command for selective auditing, refer to *Command Reference*. For more information about the **auditing** parameter, refer to *Performance Tuning*.

You can display, print, clear, and view the size of a server’s audit log. You can also write the audit log to a file and print it using NET commands. To write the first 20 entries of the audit log to a file, type at the OS/2 command line:

```
NET AUDIT /c:20 > filename
```

To view the audit log file, type:

```
TYPE filename | MORE
```

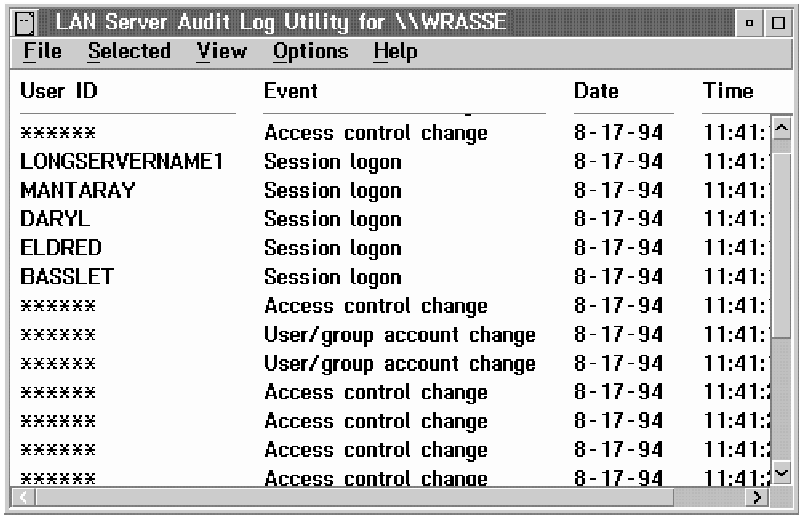
Displaying the Audit Log

Use the next procedure to see the audit log in LAN Server Administration.

To display the audit log:

1. Open **LS Audit Log Utility**.

   The Audit Log main window is displayed.



User ID	Event	Date	Time
******	Access control change	8-17-94	11:41:
LONGSERVERNAME1	Session logon	8-17-94	11:41:
MANTARAY	Session logon	8-17-94	11:41:
DARYL	Session logon	8-17-94	11:41:
ELDRED	Session logon	8-17-94	11:41:
BASSLET	Session logon	8-17-94	11:41:
******	Access control change	8-17-94	11:41:
******	User/group account change	8-17-94	11:41:
******	User/group account change	8-17-94	11:41:
******	Access control change	8-17-94	11:41:
******	Access control change	8-17-94	11:41:
******	Access control change	8-17-94	11:41:
******	Access control change	8-17-94	11:41:

Figure 7. Audit Log Main Window

2. If the desired audit log is remote:
   a. Select **Options**.
   b. Select **Select server**.

      The Select server window is displayed. It lists all available servers.
   c. Either select one of the servers or type the name of the server in the **Set server to** field.
   d. Select **OK**.

      The log for the remote server is displayed.
3. To obtain details about a particular event:
   a. Select the event.
   b. Select **Selected**.
   c. Select **Audit entry details**.

      The Audit Event Details window is displayed.

Reversing the Order of Audit Log Entries

Audit log entries are displayed in date and time order with the oldest entries displayed first. You can change the order in which entries are displayed and have the most recent entries displayed first.

To reverse the order of audit entries:

1. Open **LS Audit Log Utility**.

   The Audit Log main window is displayed.
2. If the desired audit log is remote:

   a. Select **Options**.
   b. Select **Select Server**.

      The Select Server window is displayed. It lists all available servers.
   c. Either select one of the servers or type the name of the server in the **Set server to** field.
   d. Select **OK**.

      The log for the remote server is displayed.
3. Select **View**.
4. Select **Sort**.

   The Sort Audit Log window is displayed.
5. Select the order of sorting, either **Oldest first** or **Newest first**.
6. If you want to group the sorted entries, select either **User ID** or **Audit event**.
7. Select **OK**.

Printing the Audit Log

You can print the audit log on a network printer. The audit log prints in the order selected.

To print the audit log:

1. Open **LS Audit Log Utility**.

   The Audit Log main window is displayed.
2. If the desired audit log is remote:
   a. Select **Options**.
   b. Select **Select server**.

      The Select Server window is displayed. It lists all available servers.
   c. Either select one of the servers or type the name of the server in the **Set server to** field.
   d. Select **OK**.

      The log for the remote server is displayed.
3. Select **File**.
4. Select **Print**.

   The Print File window is displayed.
5. Type the printer port name (for example, `LPT1`).
6. Select **OK**.

   The audit log for the selected server prints at the designated printer.

Writing the Audit Log to a File

Use the next procedure to store the contents of the audit log in a file.

To write the audit log to a file:

1. Open **LS Audit Log Utility**.

   The Audit Log main window is displayed.
2. If the desired audit log is remote:
   a. Select **Options**.
   b. Select **Select server**.

The Select Server window is displayed. It lists all available servers.

   c. Either select one of the servers or type the name of the server in the **Set server to** field.
   d. Select **OK**.

      The log for the remote server is displayed.
3. Select **File**.
4. Select **Output to file**.

   The Output to File window is displayed.
5. Type the name of the file where you want the audit log to be stored.
6. Select **OK**.

Clearing the Audit Log

You can clear all entries in the audit log for a specified server. After you clear an audit log, you cannot recover the entries.

To clear the audit log:

1. Open **LS Audit Log Utility**.

   The Audit Log main window is displayed.
2. If the desired audit log is remote:
   a. Select **Options**.
   b. Select **Select server**.

      The Select Server window is displayed. It lists all available servers.
   c. Either select one of the servers or type the name of the server in the **Set server to** field.
   d. Select **OK**.

      The log for the remote server is displayed.
3. Select **File**.
4. Select **Clear**.

Changing the Size of the Audit Log

You can set the size of the audit log either permanently in the IBMLAN.INI file or temporarily (as long as the server is active).

The size of the audit log is set permanently in the IBMLAN.INI file by the **maxauditlog** parameter in the Server section; refer to *Performance Tuning* for the **maxauditlog** parameter description. Each audit log entry occupies about 64 bytes. When the audit log reaches the maximum size, no more entries are recorded until the size is increased or the audit log entries are cleared.

Before you can change the size of the audit log at a server, the server must be started, and you must be logged on as an administrator.

To temporarily change the audit log size:

1. Open **LS Audit Log Utility**.

   The Audit Log main window is displayed.
2. If the desired audit log is remote:
   a. Select **Options**.

   b. Select **Select server**.

      The Select Server window is displayed. It lists all available servers.

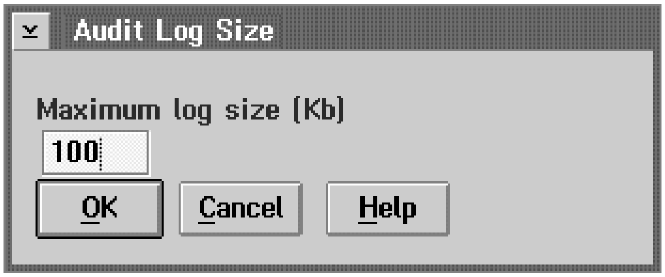
   c. Either select one of the servers or type the name of the server in the **Set server to** field.

   d. Select **OK**.

      The log for the remote server is displayed.

3. Select **Options**.
4. Select **Set maximum size**.

   The Audit Log Size window is displayed. It shows the maximum log size.



Maximum log size (Kb)
100

Figure 8. Audit Log Size Window

5. Type the new maximum size in KB. The default is 100KB.
6. Select **OK**.

Accessing Error Logs

OS/2 Warp Server or LAN Server maintains an *error log* on the system hard disk where it is installed. The error log maintains a record of problems that occurred during a network operation.

The error log contains the following information:

- Name of the service or program that generated the error
- Date and time at which the error occurred
- Number and text of the error message
- Description, or cause, of the error

You can display, sort, print, and clear error log entries and output them to a file.

For more information, see the following topics:

- “Displaying the Error Log” on page 157
- “Reversing the Order of Error Log Entries” on page 158
- “Printing the Error Log” on page 159
- “Writing the Error Log to a File” on page 159
- “Clearing the Error Log” on page 160
- “Changing the Size of the Error Log” on page 160

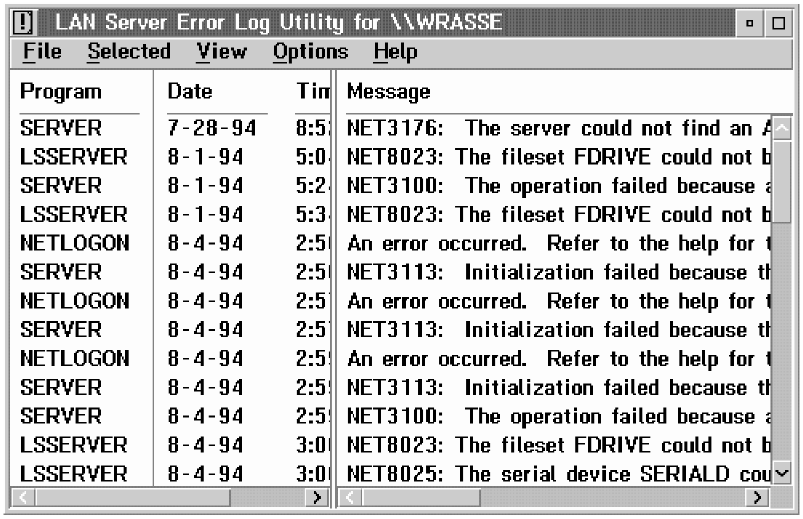
Displaying the Error Log

Use the next procedure to view the error log in LAN Server Administration.

To display an error log:

1. Open **LS Error Log Utility**.

   The Error Log main window is displayed.



Program	Date	Tim	Message
SERVER	7-28-94	8:5	NET3176: The server could not find an
LSSERVER	8-1-94	5:0	NET8023: The fileset FDRIVE could not b
SERVER	8-1-94	5:2	NET3100: The operation failed because
LSSERVER	8-1-94	5:3	NET8023: The fileset FDRIVE could not b
NETLOGON	8-4-94	2:5	An error occurred. Refer to the help for
SERVER	8-4-94	2:5	NET3113: Initialization failed because th
NETLOGON	8-4-94	2:5	An error occurred. Refer to the help for
SERVER	8-4-94	2:5	NET3113: Initialization failed because th
NETLOGON	8-4-94	2:5	An error occurred. Refer to the help for
SERVER	8-4-94	2:5	NET3113: Initialization failed because th
SERVER	8-4-94	2:5	NET3100: The operation failed because
LSSERVER	8-4-94	3:0	NET8023: The fileset FDRIVE could not b
LSSERVER	8-4-94	3:0	NET8025: The serial device SERIALD cou

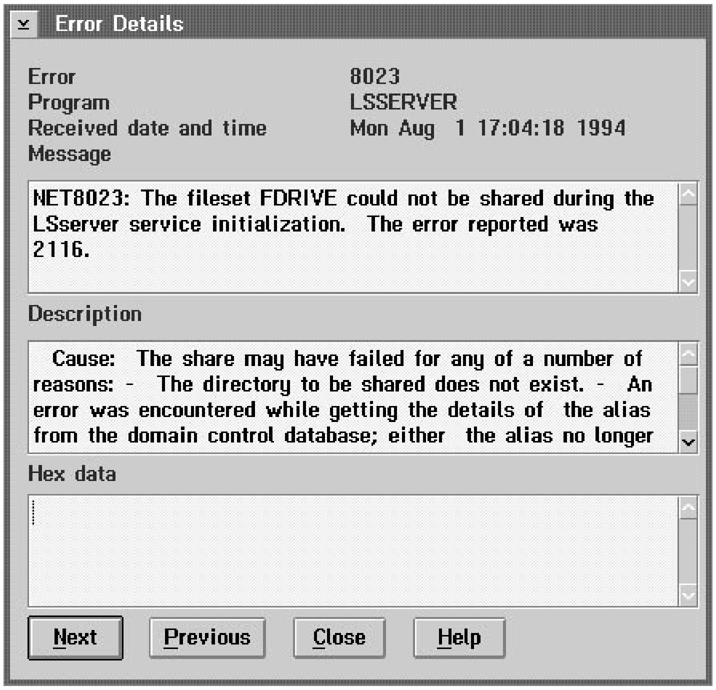
Figure 9. Error Log Main Window

2. If the desired error log is remote:
   1. Select **Options**.
   2. Select **Select server**.

      The Select Server window is displayed. It lists all available servers.
   3. Either select one of the servers or type the name of the server in the **Set server to** field.
   4. Select **OK**.

      The log for the remote server is displayed.
3. To obtain details about a particular event:
   1. Select the event.
   2. Select **Selected**.
   3. Select **Error details**.

      The Error Details window is displayed. The **Hex data** field sometimes contains additional information about an error. For example, it may contain network control block (NCB) information, a file name, or an error code.



Error 8023
Program LSSERVER
Received date and time Mon Aug 1 17:04:18 1994
Message

NET8023: The fileset FDRIVE could not be shared during the LSserver service initialization. The error reported was 2116.

Description

Cause: The share may have failed for any of a number of reasons: - The directory to be shared does not exist. - An error was encountered while getting the details of the alias from the domain control database; either the alias no longer

Hex data

Figure 10. Error Details Window

Reversing the Order of Error Log Entries

Error Log entries are displayed in date and time order with the oldest entries displayed first. You can change the order in which entries are displayed and have the most recent entries displayed first.

To reverse the order of error log entries:

1. Open **LS Error Log Utility**.

   The Error Log main window is displayed.
2. If the desired error log is remote:
   a. Select **Options**.
   b. Select **Select Server**.

      The Select Server window is displayed. It lists all available servers.
   c. Either select one of the servers or type the name of the server in the **Set server to** field.
   d. Select **OK**.

      The log for the remote server is displayed.
3. Select **View**.
4. Select **Sort**.

   The Sort Error Log window is displayed.
5. Select the order of sorting, either **Oldest first** or **Newest First**.
6. If you want to group the sorted entries, select **Group by program reporting error**.
7. Select **OK**.

Printing the Error Log

You can print the error log on a network printer. The error log prints in the order selected.

To print the error log:

1. Open **LS Error Log Utility**.

   The Error Log main window is displayed.
2. If the desired error log is remote:
   a. Select **Options**.
   b. Select **Select Server**.

      The Select Server window is displayed. It lists all available servers.
   c. Either select one of the servers or type the name of the server in the **Set server to** field.
   d. Select **OK**.

      The log for the remote server is displayed.
3. Select **File**.
4. Select **Print**.

   The Print File window is displayed.
5. Type the printer port name (for example, `LPT1`).
6. Select **OK**.

   The error log for the selected server prints at the designated printer.

You can also print the error log to a file using the NET PRINT command. For more information, refer to the *Command Reference*.

Writing the Error Log to a File

Use the next procedure to store the contents of the error log in a file.

To write the error log to a file:

1. Open **LS Error Log Utility**.

   The Error Log main window is displayed.
2. If the desired error log is remote:
   a. Select **Options**.
   b. Select **Select Server**.

      The Select Server window is displayed. It lists all available servers.
   c. Either select one of the servers or type the name of the server in the **Set server to** field.
   d. Select **OK**.

      The log for the remote server is displayed.
3. Select **File**.
4. Select **Output to file**.

   The Output to File window is displayed.
5. Type the name of the file where you want the error log to be stored.
6. Select **OK**.

Clearing the Error Log

You can clear all entries in the error log for a specified server. After you clear an error log, you cannot recover the entries.

To clear an error log:

1. Open **LS Error Log Utility**.

   The Error Log main window is displayed.
2. If the desired error log is remote:
   a. Select **Options**.
   b. Select **Select server**.

      The Select Server window is displayed. It lists all available servers.
   c. Either select one of the servers or type the name of the server in the **Set server to** field.
   d. Select **OK**.

      The log for the remote server is displayed.
3. Select **File**.
4. Select **Clear**.

Changing the Size of the Error Log

You can set the size of the error log either permanently in the IBMLAN.INI file or temporarily (as long as the server is active).

The size of the error log is set permanently in the IBMLAN.INI file by the **maxerrorlog** parameter in the Server section; refer to *Performance Tuning* for the **maxerrorlog** parameter description. Each error log entry occupies about 64 bytes. When the error log reaches the maximum size, no more entries are recorded until the size is increased or the error log entries are cleared.

With the Error Log utility, you can change the maximum size only for the current session. To change the size permanently, modify the value in the IBMLAN.INI file. Before you can change the size of the error log at a server, the server must be started, and you must be logged on as an administrator.

To change the error log size temporarily:

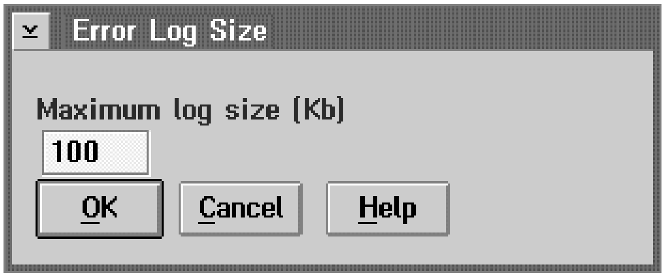
1. Open **LS Error Log Utility**.

   The Error Log main window is displayed.
2. If the desired error log is remote:
   a. Select **Options**.
   b. Select **Select server**.

      The Select Server window is displayed. It lists all available servers.
   c. Either select one of the servers or type the name of the server in the **Set server to** field.
   d. Select **OK**.

      The log for the remote server is displayed.
3. Select **Options**.
4. Select **Set maximum size**.

   The Error Log Size window is displayed. It shows the maximum log size.



Maximum log size (Kb)
100

Figure 11. Error Log Size Window

5. Type the new maximum size in KB. The default is 100KB.
6. Select **OK**.

DOS and OS/2 Command Restrictions

You can use most of the DOS commands on network disks, directories, and printers. However, you cannot use some DOS and OS/2 commands with network devices. If you try to use these commands with a network device, you receive an error message. You can use these commands with your local disks and printers.

You cannot use the following DOS commands with redirected drives:

- BACKUP
- CHKDSK (Check Disk)
- DISKCOMP (Disk Compare) – Use the COMP (Compare) command to compare files.
- DISKCOPY (Disk Copy) – Use the COPY and XCOPY commands to copy files.
- FORMAT
- JOIN
- LABEL – You cannot change the volume label of a network device you are using.
- PRINT – Use the NET PRINT (or NET COPY) command if you are using network devices.
- RECOVER
- RESTORE
- SUBST (Substitute)
- SYS
- VERIFY

The following are the only commands that you can use with universal naming convention names:

- TYPE
- PRINT

You cannot use the following OS/2 commands with redirected drives:

- CHKDSK (Check Disk)
- DISKCOPY (Disk Copy)
- JOIN
- LABEL
- RECOVER

- RESTORE
- SHELL

You cannot use the following OS/2 commands with universal naming convention names.

- BACKUP
- COPY

Managing More Than One Domain

You can manage up to six domains through LAN Server Administration. You can manage a domain from a workstation if the following conditions apply:

- Your user ID and password are defined as administrator IDs for all domains.
- One or more of the following applies:
  - The domain name is specified as your default domain name using the **domain** parameter in the IBMLAN.INI file.
  - The domain name is specified as one of four possible names in the **othdomains** parameter in the IBMLAN.INI file.
  - You are logged on at that domain.

The following is an example of how you would specify the **OTHDOMAINS** parameter in the IBMLAN.INI file:

```
OTHDOMAINS = domain1,domain2,domain3,domain4
```

You can specify up to four additional domains using the **OTHDOMAINS**parameter on the client or server on which you are logging on. After you specify additional domains, restart LAN Requester and then log on. Additional domain objects are displayed in LAN Server Administration, with which you can manage these domains. You can manage a total of six domains in LAN Server Administration if you log on to a domain that is different from your default domain.

First Failure Support Technology/2 (FFST/2)

First Failure Support Technology/2 (FFST/2) is a set of reliability, availability, and serviceability (RAS) functions that OS/2 Warp Server or LAN Server and other applications can use to perform problem determination tasks. The following list describes the functions that are provided.

Message console services
FFST/2 provides a Presentation Manager message console facility that maintains a scrollable copy of all messages logged or displayed byFFST/2. This service permits any type of process (including detached processes) to display messages on the Presentation Manager screen. The user can quickly obtain a record of recently displayed or logged messages.

Error logging
FFST/2 can construct a symptom record that uniquely identifies the error detected and place the record in the OS/2 error log.

Message logging
FFST/2 can retrieve application-specified messages from National Language Support (NLS) message files and record the messages in a log file. Optionally, FFST/2 can display the messages through the message console facility. Message display can be turned on or off through the FFST/2 initialization and configuration program.

Building and routing generic alerts
FFST/2 can be used to build and route a software generic alert to describe a detected error condition. The alert can include key segments of the symptom record built by the error logging facility if error logging has been selected.

Selective data collection and dump
FFST/2 can collect and dump storage areas and files selected by the calling application.

FFST/2 requires hardware *vital product data* (VPD) so that it can identify machines properly in the messages it generates. Vital product data includes the machine type, model number, serial number, and plant of manufacture. Vital product data and other configuration information is entered by the user at installation time.

The following tasks can be configured by the FFST/2 installation and configuration program:

- Enable or disable FFST/2
- Enable or disable the display of application messages
- Set the maximum number of dump data sets that can exist in the current directory for a given type of dump
- Set subdirectories to be used for FFST/2 dump files
- Set the FFST/2 message log path and file name

Chapter 13. Managing Local Security on 386 HPFS

Permissions that you set for a resource usually apply only to remote users accessing the resource from different workstations. Local Security is provided for the 386 HPFS and extends access restrictions to local users working at the server. It protects all files on 386 HPFS volumes of the server from unauthorized local access. Files stored on the FAT file system volumes are not protected by Local Security; however, they are still protected from remote access by unauthorized users. Administrators set permissions for all files on the server and are not subject to access control permissions.

When you are working at a server with Local Security, you can access a file only if you have adequate permissions for that file. When you run a program, the program can access a file only if you have permission to access the file. Your permissions, not those of the program, control access to files. Local NetAPI calls are also subject to privilege checking when Local Security is active. However, an administrator can also start a program and give it special privileges.

For more information, see the following topics:

- "Local Security on a 386 HPFS Server"
- "Starting a Server with Local Security"
- "Accessing Files with Local Security" on page 166
- "Running Privileged Programs at Startup" on page 167
- "Running Privileged Programs from the Command Line" on page 167
- "Local Security Guidelines" on page 168

Local Security on a 386 HPFS Server

Local Security protects files on 386 HPFS formatted volumes on the server, regardless of whether OS/2 Warp Server or LAN Server is running. When a local user tries to access a file on a 386 HPFS volume on the server, Local Security checks the permissions for the file. Access is allowed only if the user has the required permissions. Local Security also checks file permissions when you run a program that accesses files.

File-access auditing is also improved on a server with Local Security installed. Auditing of the files and directories on 386 HPFS volumes on the server begins when the workstation is started, even if the Server service is not started.

For information concerning Local Security installation, refer to *Quick Beginnings* .

Starting a Server with Local Security

When you start a server on which Local Security is installed, many programs are started. To ensure that the operating system and programs run successfully when no one is logged on to the server, give the special group LOCAL read (R) and execute (X) permissions to the files needed for the operating system and those programs.

Only administrators can start services on servers with Local Security. To help you set up correct permissions for system files,OS/2 Warp Server or LAN Server displays the following prompt when a server with Local Security is started:

```
LAN Server Local Security has started.

Press ESC to log on now, or press ENTER to
start the workstation with no one logged on.
```

Press Enter to test whether the workstation initializes itself with no one logged on. If the workstation does not start successfully, restart it and press Esc when the prompt is displayed.

Note: This prompt is automatically removed after a short while, allowing the server to start automatically without intervention. For this reason, it is recommended that the server and its desktop be allowed to start with no one logged on.

When the logon prompt is displayed, then log on using a user ID that has administrator privilege on the server. You can adjust the server file permissions for the group LOCAL if you want the workstation to start with no one logged on. For information on how to set up permissions for the group LOCAL, see “Local Security Guidelines” on page 168.

After you grant permissions for system files, log off so that no one else can use the administrator privilege on the server.

Note: If you log on locally to a server with Local Security, log on to the network, and then log off from the network, you are still logged on at the local server.

Accessing Files with Local Security

OS/2 Warp Server or LAN Server creates a special group called LOCAL on servers with Local Security. No users are members of this group nor can any users be added to it. The LOCAL group is a special group ID whose permissions are granted to the system or to users using the local system when no one is logged on. The group LOCAL does not show up in User Profile Management windows; however, it does show up in the LAN Server Administration GUI.

Users working at the server workstation when no one is logged on receive the permissions granted to the group LOCAL. If you log on with user privilege, you have the permissions granted to your own user ID and to any groups of which you are a member, in addition to the permissions granted to group LOCAL. If you log on with administrator privilege, you can access all files on the server. For more information about the logon and logoff utilities, refer to “Chapter 5. Managing Users and Groups” on page 43.

The following list provides a summary of permissions for a user working at the console of a server with Local Security:

Local user not logged on
Permissions granted to the group LOCAL, but no access to the network

Local user logged on only to a local server
Permissions granted to the group LOCAL and the user ID, but no access to the network

Local user logged on to the network
Permissions granted to the group LOCAL, the user ID, and access to the network

Note: Both the user ID and corresponding password must be in the accounts database for the server running Local Security before OS/2 Warp Server or LAN Server will grant network permissions. If OS/2 Warp Server or LAN Server does not find a valid user ID, OS/2 Warp Server or LAN Server grants only the permissions of the group LOCAL at the local server.

Running Privileged Programs at Startup

Many programs must have access to all the files on the server. Only the administrator can start and run a program as a *privileged* program that can access all files on the server whether or not anyone is logged on locally.

An administrator has two ways to start a privileged program when the workstation starts:

- Edit the PRIVINIT.CMD file to add the command that starts the program. The PRIVINIT.CMD file is a special batch program, located in the root directory on the startup drive, that runs when a workstation with Local Security starts. Each command in the PRIVINIT.CMD file starts as a privileged program.

  Note: Starting the PRIVINIT.CMD file by itself does not make the programs in the PRIVINIT.CMD file privileged. Start the PRIVINIT.CMD file by specifying the RUNPRIV.EXE file in the STARTUP.CMD file.

  Commands in the PRIVINIT.CMD file are not automatically run as background programs. To start a background program from the PRIVINIT.CMD file, use the DETACH statement. For more information about the DETACH statement, see your operating system documentation.
- Put the command to start the program in the CONFIG.SYS file using the RUN statement. Programs started with the RUN statement always are started as background programs. For more information about the RUN statement, see your operating system documentation.

Commands in the STARTUP.CMD file are not run as privileged programs. Therefore, you must be logged on locally as an administrator to start OS/2 Warp Server or LAN Server services from the STARTUP.CMD file.

Note: To start a service automatically when the server starts and before anyone logs on at the server, put the NET START command (with the service to be started) in the PRIVINIT.CMD file.

Running Privileged Programs from the Command Line

To start a privileged program at the OS/2 command prompt after the server is running, type `PRIV` followed by the command to start the program.

For example, to start the SORT program in the background, type:

```
DETACH SORT <source> target
```

To start the SORT program as a privileged background program, type:

```
DETACH PRIV SORT <source> target
```

Note: OS/2 Warp Server or LAN Server services are an exception to this requirement. When started, OS/2 Warp Server or LAN Server services are automatically treated as privileged programs. The PRIV command is not needed.

When you start a program as a privileged program, the privilege applies only to that instance of the program. If you or another user runs the program again later, the program is not automatically privileged. This restriction applies to privileged programs started both from the command line and by the PRIVINIT.CMD file.

Programs started by a privileged program, regardless of how the privileged program was started, are also privileged. See the *Command Reference* for more information on the PRIV utility.

Refer to *Performance Tuning* for more information about how to set up the CONFIG.SYS file for Local Security.

Local Security Guidelines

On a server with Local Security, restrictions begin when the workstation starts, before system initialization files run. If you want the workstation to initialize when no one is logged on, the group LOCAL must have permission to run the server startup programs.

To accomplish this, the installation/configuration program automatically grants local permissions for certain files when local security is installed. Refer to “Default Access Control Profiles on Servers” on page 97 for a list of permissions installed with Local Security.

Once OS/2 Warp Server or LAN Server is installed, you can modify the default permissions. However, when you set permissions for any files on a server with Local Security, follow the security guidelines for each type of file.

For more information, see the following topics:

- “System Files”
- “Data Files” on page 169
- “Executable Programs and Dynamic Link Libraries” on page 169
- “NET.ACC File” on page 169
- “Local Security Considerations for Programs” on page 170

System Files

The following files are examples of system files:

CONFIG.SYS
PRIVINT.CMD
STARTUP.CMD
IBMLAN.INI
SECURESH.EXE

The changes for the OS/2 operating system require that the desktop directory and files specified by the environment variables USER_INI and SYSTEM_INI have R, W, and X permissions for the entire tree. These permissions allow the desktop to start properly, but not all programs within the desktop can run without at least one user being logged on. If this is unacceptable in your environment, set up the server so that someone logs on during startup.

Data Files

Data files are classified in three types: public, program, and private.

Use the following security guidelines to set permissions for data files:

- Give all local users read permission to public data files.
- Give all local users read and write permissions to program data files written to by programs that all users are allowed to use.
- Do not give any permissions to the private user data files to the group LOCAL. Give permissions for these private data files only to the appropriate users.

Executable Programs and Dynamic Link Libraries

Executable programs have .EXE and .DLL as file name extensions. A dynamic link library contains commands used by executable programs.

Use the following security guidelines to set permissions for executable programs and dynamic link libraries:

- For general-use programs, give read and execute permissions to local users as long as the permissions for the data files modified by these programs are set correctly.
- For programs and dynamic link libraries used only by administrators, do not give permissions to local users or to any other group.
- Do not give write or delete permissions for any program or dynamic link library.
- Do not give create permission for any directory specified in the PATH statement in the CONFIG.SYS file.

NET.ACC File

The NET.ACC file contains the user accounts database for the server.

Use the following security guidelines to set permissions for the NET.ACC file:

- The installation/configuration program gives all local users read, write, and execute permissions to the NET.ACC file.

  Giving the group LOCAL read, write, and execute permissions should not cause security problems since the account information in the NET.ACC file is stored in binary format instead of ASCII text. Therefore, the information is not easily readable with a text editor.

  Also, as long as Local Security for 386 HPFS is enabled, the NET.ACC file remains open. Commands and programs that need exclusive access to a file cannot work on the NET.ACC file while OS/2 Warp Server or LAN Server is running. The COPY and DEL commands, for example, need exclusive access.
- If you revoke the read, write, and execute permissions for the NET.ACC file, a local user cannot change a password or user comments while working at the server; however, a user could do so from a remote workstation.

Notes:

1. The NETACC.BKP file is the NET.ACC backup file created by the BACKACC utility. In order to preserve the NETACC.BKP file, do not give any users or groups access permissions to the NETACC.BKP file.
2. In order to run the BACKACC command on a machine installed with Local Security, you must:
   - Be logged on locally as an administrator
   - Have access to the \IBMLAN\ACCOUNTS subdirectory
   - Have access to the root directory of the current drive

Local Security Considerations for Programs

On servers with Local Security, all programs are subject to file-access permissions. All programs have the permissions granted to the group LOCAL. In addition, when a user logs on locally at the server, each program the user runs has the permissions granted to that user. When an administrator logs on, each program the administrator runs can access all files on the server, just as the administrator can.

While one or more programs are running, users can log on and off the server. If a program is not privileged and a user or administrator logs on at the server, that program has the privilege of the user or administrator. When the user or administrator logs off at the server, the program has the privileges provided by the group LOCAL.

For more information, see the following topics:

- “Local Security Error Messages”
- “Local Security Access Control Profiles”

Local Security Error Messages

If users have problems running programs that are normally accessible, the problems might be caused by Local Security securing the file system. In some applications and programs, error messages do not clearly indicate that the cause of the problem is that users do not have sufficient access permissions to files on the locally secured workstation.

To see if Local Security is preventing access because of insufficient access permissions for a user ID, log on to the workstation using an administrator ID and try the command again. Administrators can access all programs on a workstation with Local Security. If necessary, provide the needed access permissions to the group LOCAL or to users requiring access to programs on the workstation.

Note: Turn on auditing to highlight problems with Local Security and file access. If administrators can successfully run programs but users cannot, turn on auditing for both the server and the resources in question. Local resources are audited if Local Security is running.

Local Security Access Control Profiles

The following example illustrates the access control profiles that are added to servers when Local Security is installed:

```
For all subdirectories specified          LOCAL:RX
by the DPATH environment variable
For all subdirectories specified          LOCAL:RX
```

by the PATH environment variable	
For all subdirectories specified by the LIBPATH variable in CONFIG.SYS	LOCAL:RX
For all subdirectories specified by the DESKTOP directory tree	LOCAL:RWX
For all subdirectories specified by the GLOSSARY environment variable	LOCAL:RX
For all subdirectories specified by the BOOKSHELF environment variable	LOCAL:RX
For the file referenced by the USER_INI environment variable	LOCAL:RWX
For the file referenced by the SYSTEM_INI environment variable	LOCAL:RWX
For all subdirectories specified by the TMP environment variable	LOCAL:RWXCD
For all subdirectories specified by the TEMP environment variable	LOCAL:RWXCD
x:\	LOCAL:RX
Other HPFS drive roots	LOCAL:RX
x:\OS2	LOCAL:RX
x:\IBM386FS	LOCAL:RX
x:\OS2\INSTALL	LOCAL:RX
x:\OS2\HELP	LOCAL:RX

DBCS Note: The following access control profile is added only for DBCS systems:

x:\OS2\SYSDATA	LOCAL:RWX

x:\OS2\BOOK	LOCAL:RX
x:\OS2\DLL	LOCAL:RX
x:\OS2\SYSTEM	LOCAL:RX
x:\SPOOL and subdirectories (queues)	LOCAL:RWXCDA
x:\IBMCOM	LOCAL:RX
d:\IBMLAN	LOCAL:RX
d:\IBMLAN\BOOK	LOCAL:RX
d:\IBMLAN\ACCOUNTS	LOCAL:RX
d:\IBMLAN\LOGS	LOCAL:RX
d:\IBMLAN\ACCOUNTS\NET.ACC	LOCAL:RWX
d:\IBMLAN\ACCOUNTS\NETACC.BKP	LOCAL:NONE
d:\IBMLAN\NETLIB	LOCAL:RX
d:\IBMLAN\NETPROG	LOCAL:RX
x:\IBM386FS\HPFS386.IFS	LOCAL:NONE
d:\IBMLAN\INSTALL	LOCAL:NONE
d:\IBMLAN\SERVICES	LOCAL:RX
x:\MUGLIB	LOCAL:RX
x:\MUGLIB\ACCOUNTS	LOCAL:RX
x:\MUGLIB\DLL	LOCAL:RX
x:\OS2\MDOS\WINOS2\SYSTEM	LOCAL:RX
x:\OS2\MDOS\WINOS2\*.INI	LOCAL:RWX
x:\OS2\MDOS\WINOS2\*.GRP	LOCAL:RWX
x:\NOWHERE	LOCAL:RWX

where *x* is the drive from which the OS/2 operating system was started and *d* is the drive where the subdirectory is located.

Notes:

1. The default access control profiles for Local Security permit the default OS/2 desktop to start for users if no one is logged on. If the desktop has been reconfigured, not all of the correct access control profiles might be created. If the desktop cannot be started when no one logs on, try logging on as an administrator. Then verify that all of the objects referred to during the desktop initialization display correctly.
2. The DESKTOP and NOWHERE directory names can be different on other machines. For example, the OS/2 2.0 desktop can be renamed to

MYDESKTOP. In this case, MYDESKTOP should have LOCAL:RWX access. The NOWHERE directory name is translated for different languages.

Chapter 14. Using Fault Tolerance

The Fault Tolerance system, provided with 386 HPFS, protects against data loss due to hard-disk failure by:

- Maintaining two copies of the data.
- Monitoring hard-disk operations.
- Correcting some errors automatically.
- Alerting an administrator about errors that cannot be automatically corrected

The Fault Tolerance system allows drive mirroring and drive duplexing as well as error logging, alerting, and monitoring of disk activity in a mirrored, duplexed, or standard server disk system. Fault Tolerance can be installed on any server using 386 HPFS and can be administered remotely. In some cases, read performance can be improved for disks on mirrored drives, as the disk with the least number of items waiting for I/O is chosen for the read request.

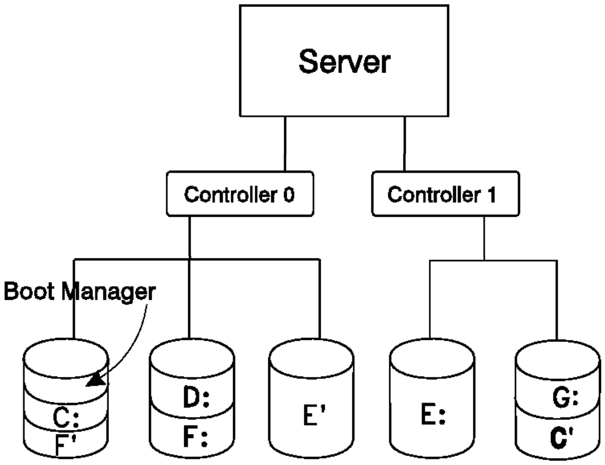


Figure 12. Fault Tolerance Drive Scenario

Drive mirroring and drive duplexing provide duplication of data stored on disk, thereby improving data integrity. *Drive mirroring* is the duplication of a single logical drive or volume on two partitions, primary and secondary, that do not reside on the same physical disk. If the data on the two partitions differs, the drives are synchronized through *drive verification*, which ensures that the drives are identical.

The *primary partition* is visible to the operating system. A primary partition as used within the Fault Tolerance system should not be confused with a primary partition as used by Logical Volume Manager (LVM). Fault Tolerance primary partitions are actually *logical partitions* in LVM. The *secondary partition* is the backup partition and is not visible to the operating system. The mirroring process automatically creates secondary partitions from contiguous free space. In the previous figure, drive F is mirrored. Drive F is the primary partition and F’ (F prime) is the secondary partition.

Drive duplexing is a special type of drive mirroring, with the additional advantage that the two disks on which the two partitions reside are controlled by two different disk controllers. Drive duplexing provides protection against errors caused by a faulty controller as well as errors caused by a faulty disk. In the previous figure, drives C and E are duplexed. Drives C and E are primary partitions and C’ and E’ are secondary partitions.

Drive mirroring requires a minimum of two physical disks. The disks you use for mirroring must have the same geometry. Disks with matching geometries have the same number of sectors per track and the same number of tracks per cylinder. Drive duplexing requires a minimum of two disks on two different controllers. In addition, each mirrored pair of partitions must reside on disks that are handled by the same disk device driver.

Fault Tolerance supports up to 48 hard-disk partitions (24 mirrored drives).

Fault monitoring detects and logs errors that occur during hard-disk read and write operations. If you are monitoring disk operations, you’ll receive an alert when a critical error occurs.

Error correction helps recover and restore data that is otherwise lost because of a disk error. When certain disk errors occur, HPFS automatically recovers the data through *hotfixing*. Hotfixing detects bad sectors and reroutes data to a good sector in a reserved area on the drive. Hotfixing is automatic and works only on a drive with HPFS. The hotfix corrects both the primary and secondary partitions, but it is not audited or in any other way supported by the Fault Tolerance Monitor Utility (FTMONIT).

Another form of error correction is performed by the FTMONIT during system startup if disk errors are indicated by either a disk failure or a low-confidence compare failure. A low-confidence compare failure occurs when Fault Tolerance discovers that key data structures on both partitions of a mirrored disk do not match. If disk errors are indicated, the FTMONIT utility automatically attempts to verify or compare all sectors on both the primary and secondary partitions of mirrored drives and correct any inconsistencies or errors. A message is displayed indicating the drive that is being verified. During the verification, the disk is locked and unavailable to users.

Fault monitoring is possible regardless of the number of disks in the workstation and whether they are mirrored, duplexed, or neither. Fault Tolerance is available only for LVM compatibility volumes.

For more information, see the following topics:

- “Fault Tolerance Utilities”
- “Getting Started” on page 175
- “Creating Logical Drives (Compatibility Volumes)” on page 176
- “Starting Fault Tolerance Using the FTSETUP Utility” on page 177
- “Using the FTADMIN Utility” on page 183
- “Using the FTREMOTE Utility” on page 192
- “Fault Tolerance Recovery Procedures” on page 193

Fault Tolerance Utilities

The following four utilities control Fault Tolerance:

- The Fault Tolerance Setup (FTSETUP) utility is used to configure Fault Tolerance and to mirror drives. Refer to "Starting Fault Tolerance Using the FTSETUP Utility" on page 177 for more information about using theFault Tolerance Setup utility.
- The FTMONIT utility controls Fault Tolerance monitoring and reports errors. By default, errors are logged and administrators are alerted about errors. The FTMONIT utility runs automatically when the line `RUN=FTMONIT.EXE` is added to the CONFIG.SYS file. This line is automatically added to the CONFIG.SYS file when you run the FTSETUP utility the first time. Because the FTMONIT utility runs automatically in the background, this chapter does not describe how to use this utility. Refer to *Command Reference* for more information.
- The Fault Tolerance Administration (FTADMIN) utility displays the Fault Tolerance error log, manages Fault Tolerance on remote servers, views drive statistics, and manage error correction and drive verification. The FTADMIN utility can be run remotely to perform these tasks on other server workstations on which the user has administrative privileges. Refer to "Using the FTADMIN Utility" on page 183 for more information.
- The Fault Tolerance Remote (FTREMOTE) utility is a response-file-driven version of the FTADMIN utility and the FTSETUP utility that activates Fault Tolerance, configures the drives to use Fault Tolerance in an unattended state, verifies mirrored drives, and corrects errors. the FTREMOTE utility can be called from the command line, from within a batch file, or through a software distribution manager (SDM) such as the LAN configuration, installation, and distribution Utility (LAN CID Utility). Refer to *Command Reference* for more information.

Note: To use Fault Tolerance, Fault Tolerance Support must be installed on at least one server. In addition, Fault Tolerance Administration can be installed on clients so that administrators can then correct errors remotely.

Getting Started

The general steps to getting started with Fault Tolerance are as follows:

1. Install OS/2 LAN server and Fault Tolerance. Select the Tailored path during installation to find the option for installing Fault Tolerance. You must install Fault Tolerance support on at least one server. In addition, you can install the FTADMIN utility on clients. With the FTADMIN utility, administrators can correct errors remotely.

   Note: To use FTADMIN remotely, first copy the following files from the server to the client:

   - IBMLAN\NETPROG\FTMONIT.EXE
   - IBMLAN\NETPROG\FTADMIN.HLP
   - IBMLAN\NETPROG\FT.DLL
2. Use LVM to create the logical drives to be used as Fault Tolerance primary partitions on each disk. Secondary partitions are created for you when you mirror the primary partitions. The mirroring process also automatically formats both the primary and secondary partitions for the 386 HPFS.

   Note: Define all partitions with LVM. Then use the FTSETUP utility, not LVM, to manipulate the drives.
3. If you plan to mirror the boot drive, create it as a logical partition and install boot manager.

4. Use the FTSETUP utility to mirror drives that contain critical applications and data. Up to 24 drives can be mirrored, depending on available disk space and the number of primary partitions.
5. Update your 386 HPFS Utility Disk 2 with the new mirroring configuration.
6. Designate one or more administrators to receive alerts. Add the administrator user IDs to the **alertnames** parameter in the IBMLAN.INI file.
7. Maintain a regular disk backup schedule. Fault Tolerance provides protection for single disk failures; however, Fault Tolerance does not necessarily provide protection for multiple failures or failures that occur on both partitions of a mirrored drive.

For more information, see the following topic:

- "Planning Example"

Planning Example

Using Figure 12 on page 173 as a guide, the following example illustrates how you can plan for using Fault Tolerance.

Your company requires continuous server availability during business hours. Some of the data kept at the server must be available at all times. Other data is needed only occasionally. You decide to organize the server by placing programs and data on separate drives, as follows:

- The C drive is the startup drive, containing OS/2, OS/2 Warp Server, and other programs used daily.
- The D drive contains correspondence and weekly sales reports, not critical to daily use.
- The E drive contains inventory and daily sales. This drive must be available during business hours.
- The F drive contains employee records, business accounting programs, customer database, useful during business hours.
- The G drive contains occasional-use software and data.

Drives C and E, needed daily, require the greatest level of protection. These drives are duplexed, providing protection from the failure of a single disk and failure of a disk controller.

Drive F, somewhat less critical, is mirrored. Drives D and G, because they are not critical to the daily running of your business, remain unmirrored. Additionally, the Boot Manager is installed to help with recovering from a failure of the C drive.

Creating Logical Drives (Compatibility Volumes)

Before you begin mirroring, you need to create a logical drive (a logical partition and a compatibility volume in LVM) to serve as a Fault Tolerance primary partition. You need to create only the drives you want to mirror. You do not need to create a drive for secondary partitions.

Attention: Do not use LVM to delete a drive that is mirrored. Refer to "Deleting a Drive" on page 182 for information about deleting a drive.

To create a logical partition:

1. Open the LVM GUI.
2. Select **Partition** from the toolbar.
3. Choose the disk for the partition.
4. Specify the size, name, location, and type of the partition.

   You must specify the type as **Logical**.
5. Select **Ok**.

To create a compatibility partition:

1. Open the LVM GUI.
2. Select **Volume**.
3. Select **Create a volume**.
4. Select **Create a non-bootable volume**.

   Note: Bootable volumes can be mirrored, but before doing this, you must install Boot Manager. For information on Boot Manager, see *Quick Beginnings*.
5. Select **Create a compatibility volume**.
6. Choose the disk for the volume.
7. Specify the name, drive letter, and size of the volume.

   The logical partition you created should appear in the partition field.
8. Select **Ok**.

Starting Fault Tolerance Using the FTSETUP Utility

The Fault Tolerance Setup (FTSETUP) utility is a Presentation Manager application that is used to configure Fault Tolerance and to mirror drives. You can start the FTSETUP utility from either LAN Server Administration or the OS/2 command line.

Before running the FTSETUP utility, drives to be mirrored must be created with LVM. Refer to "Creating Logical Drives (Compatibility Volumes)" on page 176 for basic information about LVM.

Note: Run the FTSETUP utility when disk activity is minimal.

The FTSETUP utility enables the user to:

- Activate Fault Tolerance, including fault monitoring
- View drive details
- View available disk space
- Mirror a drive
- Unmirror drives
- Delete drives
- Recover detached secondary partitions
- Rejoin two partitions into a mirrored drive
- Deactivate Fault Tolerance

For information about the main elements of the FTSETUP window, see "FTSETUP Main Window Elements" on page 178.

Activating Fault Tolerance with the FTSETUP Utility

This procedure needs to be performed only once, after installation. If, however, you install multiple operating systems, activate Fault Tolerance on all startup partitions.

Attention: Restarting the workstation or turning it off while the FTSETUP utility is running can produce unpredictable results. Always run Shutdown before restarting the workstation.

To start the FTSETUP utility from LAN Server Administration, perform the following procedure.

To activate Fault Tolerance:

1. Open **FTSETUP**.

   Note: You can, instead, start the FTSETUP utility from the command line by entering `FTSETUP` at an OS/2 prompt.

   The first time you start the FTSETUP utility, the System Capabilities window is displayed to indicate that the workstation supports either fault monitoring only or both fault monitoring and drive mirroring.
2. Select **Activate** to configure Fault Tolerance.

   Lines are added to the CONFIG.SYS file to invoke the Fault Tolerance device driver and activate fault monitoring. After the configuration is complete, an information window is displayed, indicating that the workstation must be restarted.
3. Select **Ok** on the information window.
4. Select **Drive**, and then select **Exit**.
5. Run Shutdown from the desktop. Then press Ctrl+Alt+Del to restart the workstation.

FTSETUP Main Window Elements

The main window of FTSETUP provides important information regarding the drives used for Fault Tolerance. There are four columns of information:

- The **Drive** column contains a letter, C through Z, which represents the current logical drive being viewed, or a question mark (?) for detached drives.

  The **Drive** column includes several icons:
  - An icon that looks like a drive identifies a drive that is not mirrored.
  - An icon that looks like two stacked drives identifies a drive that is mirrored.
  - An icon that looks like a cracked drive with a question mark identifies a detached drive.
- The **Volume** column contains the partition name assigned by the user to each logical drive.
- The **Status** column contains the current status of the logical drive or partition. The **Status** column can have the following values:
  - `Cannot mirror` is assigned to an unmirrored drive when there is not enough additional disk space in the workstation to mirror that drive. This value is assigned to all drives if the workstation has only a single hard disk. Also, primary partitions that are not located at the beginning of a disk cannot be mirrored.

- `Not mirrored` indicates that a drive is not mirrored and is available for drive mirroring or deleting.
- `Mirrored` indicates that the drive is mirrored and is available for drive unmirroring.
- `Detached` indicates that a mirror (secondary partition) is no longer associated with a primary partition. Any partition with this status has a question mark (?) assigned to it as a drive letter.
- `Pending mirror` indicates that the drive has been selected for mirroring and is associated with a secondary partition. The drive becomes mirrored when the workstation is restarted.
- `Pending unmirror` indicates that the drive has been selected to be unmirrored. The associated secondary partition is available as a valid logical drive. The drive becomes unmirrored when the workstation is restarted.
- `Pending recover` describes a detached drive selected for recovery. The drive is recovered when the workstation is restarted.
- `Recover/mirror` describes a detached secondary partition has been recovered and mirrored again. The newly mirrored drive is available when the workstation is restarted.

Viewing Drive Details

The **Details** menu choice on the Drive pull-down menu in the FTSETUP utility displays the details of a drive on the workstation.

To view details of a drive:

1. Select the drive for which you want to view details.
2. Select **Drive** from the menu bar of the Fault Tolerance Setup main window.
3. Select **Details**. The Drive Details window is displayed, with the following fields:
   - **Drive Letter** indicates the current leter assigned to this drive
   - **Volume name** indicates the partition name assigned by the user to the logical drive.
   - **Status** indicates the current status of the logical drive or partition.
   - **Drive format** indicates the file system type. The possible values are FAT, HPFS, and UNKNOWN.
   - **Drive size** indicates the size, in megabytes, assigned by the user when the drive was defined using LVM.
   - **Primary partition disk** indicates the number of the hard disk on which the logical drive resides (from 1 through 128).
   - **Primary starting cylinder** indicates the starting cylinder of the primary partition on the primary disk.
   - **Secondary partition disk** indicates the number of the hard disk on which the secondary partition resides. This field applies only to a mirrored drive.
   - **Secondary starting cylinder** indicates the starting cylinder of the secondary partition on the secondary disk (the disk containing the mirror). This field applies only to a mirrored drive.
4. Select **Ok** to exit the Drive Details window and return to the Fault Tolerance Setup main window.

Viewing Available Disk Space

You can view the current disk space on your system, either as a summary or as a detailed map of locations available for mirroring.

To view available disk space:

1. Open **FTSETUP**.
2. Select **Options**.
3. Select **Available Space**.
4. Select **Available Space Summary** for a brief summary of disk space or **Available Space Details** for a detailed map of disk space.

Mirroring a Drive

Mirrored drives must meet several conditions:

- They must be LVM logical partitions residing on compatibility volumes.
- A workstation must contain two or more hard disks to have mirrored partitions. The disks must have the same geometry, which is the same number of sectors per track and the same number of tracks per cylinder. Diskette drives, CD-ROM drives, removable media drives, and redirected network drives cannot be mirrored.
- The hard disk intended to contain the secondary partition must have at least as much contiguous unallocated space as the primary partition.
- If a drive contains data, the drive is formatted with HPFS. Drives formatted with the FAT file system must be reformatted with HPFS before mirroring. Back up the drive before mirroring it, because the FTSETUP utility automatically reformats the disk (after verification) and overwrites data.
- Whenever you change the configuration of a mirrored drive, you must restart the workstation to put the change into effect.
- You must update Utility Disk 2 with the latest configuration information.

Note: The FTSETUP utility automatically formats non-HPFS drives. Before mirroring drives, back up any data on non-HPFS drives. An HPFS drive containing data can be mirrored without first backing up the data it contains. If a drive is an HPFS drive and contains data, no format is done on the primary partition of the mirror. Rather, the data is directly copied to the secondary partition to create the mirror.

To mirror a drive:

1. Create the logical drive you want to mirror, if it is not already created.
2. Open **FTSETUP**.
3. Select the drive you want to mirror.
4. Select **Drive**.
5. Select **Default Location** to have Fault Tolerance select the location of the mirror or select **Select Location** to select a specific location for the mirror.
6. If you chose to specify the mirror location, the Select Mirror Location window is displayed. Highlight the location for your mirror and select **Ok**.

   Note: The following two steps apply only to those drives not already formatted with the HPFS.

7. A warning message appears if you are trying to mirror non-HPFS drives. Either select **Format** to format and mirror the drive, or select **Cancel** to cancel the mirror request.

   When the drive is formatted, the Volume Label window opens. You can, if you choose, enter a new volume label.
8. Type a volume label for the drive, and then select **Ok** on the Volume Label window.

   Note: A `Locked Drive` message might be displayed, indicating some application files are in use. Ignore this message and select **Mirror** to continue.

   An information window is displayed, indicating that the selected drive has the `Pending mirror` status.
9. Select **Ok** on the information window.

   Repeat steps 5 through 10 for additional mirrors. After finishing your selections, you must exit the FTSETUP utility and restart your workstation to use the mirrored drive.

To exit the FTSETUP utility,restart your workstation, and update Utility Disk 2:

1. Select **Drive**.
2. Select **Exit**.
3. Select **Save** from the Partition Changes window to save the changes. An information window is displayed, indicating that the FTSETUP utility is creating partition configuration files.

   Another window is displayed, indicating that data is being copied for each pending mirrored drive.
4. Run Shutdown from the desktop. When the shutdown procedure has completed, press Ctrl+Alt+Del to restart the workstation.
5. Insert Utility Disk 2 in the diskette drive.
6. From an OS/2 command prompt, copy C:\FTCFG.SYS to the A:\ drive (where A is the letter of your diskette drive).

   This updates the mirroring configuration on Utility Diskette 2.

Hints and Tips on Mirroring a Startup Drive

When you begin to mirror the startup drive, you may receive an attention message notifying you that because other processes are using the startup drive, the mirror to be created might not initially be identical to the original partition. Also, when Shutdown starts, any data in the disk cache that is intended for the startup drive is written only to the primary partition of the mirror.

When you restart, Fault Tolerance detects the difference and generates an error code 107 (a low-confidence compare error). Run the FTADMIN utility at this point and verify the mirrored startup drive. Doing so synchronizes both partitions in the mirror and corrects the error code 107.

Unmirroring a Drive

Unmirroring a drive allows for the separation of primary and secondary partitions into two separate logical drives or the deletion of the secondary partition. Use the following procedure to unmirror a drive.

To unmirror a drive:

1. Open **FTSETUP**.
2. Select the drive you want to unmirror.
3. Select **Drive**.
4. Select **Unmirror**.

   You have the option now to keep or delete the secondary partition. If you choose to keep the secondary partition, you'll be asked to provide a drive letter and volume name for it.

   An information window is displayed indicating that the unmirroring is complete.
5. Select **Ok** from the information window, exit out of FTSETUP, and restart your system to activate the changes.

Deleting a Drive

You can use the FTSETUP utility to delete any drives that are not mirrored, except for the IPL volume.

Note: If you wish to delete a drive that is currently mirrored, you must first unmirror the drive. See "Unmirroring a Drive" on page 181 for more information.

Attention: Deleting a drive causes all data on the drive to be lost. Save any valuable data on the drive before deleting the drive.

To delete a drive:

1. Open **FTSETUP**.
2. Select the drive you want to delete.
3. Select **Drive**.
4. Select **Delete**.

   An information window is displayed, indicating that deleting the drive erases all the data on that drive. Select **Ok** to continue or **Cancel** to quit.
5. An information window is displayed informoring you that drive deletion is complete. Select **Ok** on the window, exit FTSETUP, and restart your system to activate the changes.

Recovering a Detached Secondary Partition

In a mirrored pair, a secondary partition that does not have an associated primary partition is referred to as *detached*. Detached drives have a question mark (?) as their drive letter in the Fault Tolerance Setup and Fault Tolerance Administration main windows. For example, if you have a mirrored drive and the hard disk with the primary partition fails and needs to be replaced, an error is logged and an alert is sent. Data is not lost. The next time the FTSETUP utility or the FTADMIN utility is run, a question mark (?) is displayed as the drive letter for the secondary partition. The ? indicates that the secondary partition is detached. Detached drives can be a symptom of total disk failure. If you suspect total disk failure, see "Fault Tolerance Recovery Procedures" on page 193.

You can recover the detached secondary partition, making it visible to the operating system. As a part of the recovery process, the detached secondary partition optionally can be made into a primary or secondary partition of a mirrored drive.

To recover a detached drive:

1. Open **FTSETUP**.

2. Select the detached drive you want to recover.
3. Select **Drive**.
4. Select **Recover secondary**.
5. Select the type of recovery:
   - **Leave the drive unmirrored**
   - **Make the drive the primary of a mirror**
   - **Make the drive the secondary of a mirror**
6. Specify a new drive letter and partition name for the recovered partition.

   An information window is displayed, indicating that the partition has been recovered.
7. Select **Ok** from the information window, exit FTSETUP, and restart your system to activate the changes.

Rejoining Two Partitions

Fault Tolerance can rejoin two previously mirrored partitions (primary and secondary) into one mirrored drive.

To rejoin two partitions:

1. Open **FTSETUP**.
2. Select either the primary or detached secondary partition from the main window.

   Select the partitions that contains the non-corrupted data.
3. Select **Ok** to rejoin the partitions.

   An information window is displayed informing you that the two partitions have been rejoined.
4. Select **Ok** from the information window, exit FTSETUP, and restart your system to activate the changes.

Deactivating Fault Tolerance using the FTSETUP Utility

Deactivating Fault Tolerance removes some code lines from the CONFIG.SYS file, unmirrors all mirrored or pending drives and their secondary partitions, and recovers all detached secondary partitions.

To deactivate Fault Tolerance:

1. Open **FTSETUP**.
2. Select **Options**.
3. Select **Deactivate Fault Tolerance...**.
4. Select **Deactivate**.
5. Exit **FTSETUP** and restart your system.

Using the FTADMIN Utility

The Fault Tolerance Administration (FTADMIN) utility is a Presentation Manager application that is used to display the Fault Tolerance error log, display drive statistics, and control error correction and drive verification. You can start the FTADMIN utility from either LAN Server Administration or the OS/2 command line.

You can use the FTADMIN utility on any client or server workstation that is running OS/2 Warp Server. Also, you can run the FTADMIN utility remotely to perform the previously listed tasks on other server workstations on which you have administrative privileges.

From the Fault Tolerance Administration main window, you can:

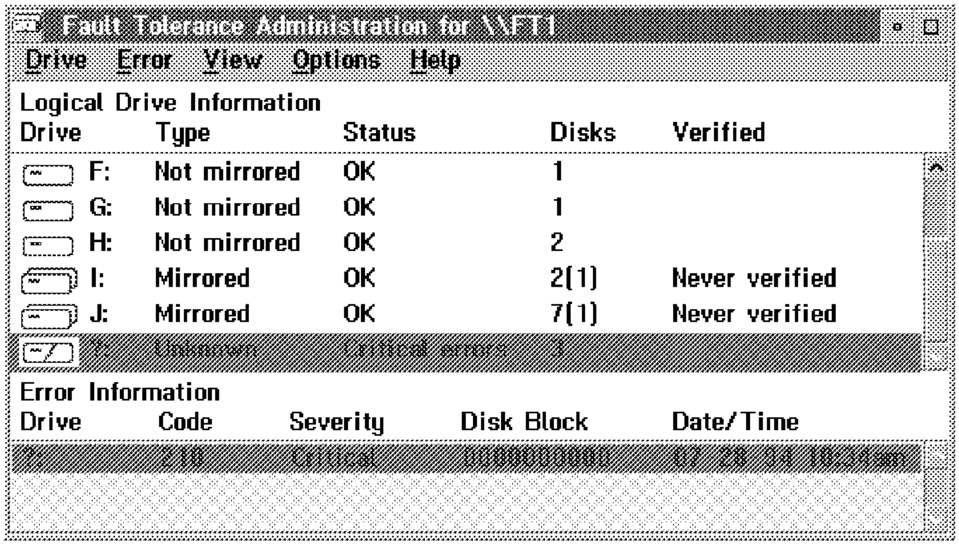
- Select a different server to administer
- Set and reset Fault Tolerance alerting
- View drive statistics
- View information about logical drives
- Sort error-rate statistics
- Display and correct disk faults
- Verify mirrored drives

For information about the main elements in the FTADMIN window, see “FTADMIN Main Window Elements”. FTADMIN can also be run remotely. See “Running the FTADMIN Utility Remotely” on page 192 for more information.

FTADMIN Main Window Elements

The Fault Tolerance Administration main window contains three sections of information:

- Title Bar
- Logical Drive Information
- Error Information



Logical Drive Information

Drive	Type	Status	Disks	Verified
F:	Not mirrored	OK	1	
G:	Not mirrored	OK	1	
H:	Not mirrored	OK	2	
I:	Mirrored	OK	2(1)	Never verified
J:	Mirrored	OK	7(1)	Never verified
?:	Unknown	Critical errors	3	

Error Information

Drive	Code	Severity	Disk Block	Date/Time
?:	210	Critical	0000000000	07 28 94 10:24am

Figure 13. Fault Tolerance Administration Main Window

For more information, see the following topics:

- “Logical Drive Information” on page 185
- “Error Information” on page 185

Logical Drive Information

The drive information section contains an icon for each of the workstation's logical drives. Diskette drives and redirected drives are not shown. When you select **Full drive information** from the View pull-down menu, the drive information section expands horizontally to show a row of detailed information about each logical drive.

Each row of information describes a logical drive. An icon that represents the drive and its current state heads the row. The various icons and their meanings are as follows:

- An icon that looks like a drive identifies a drive that is not mirrored.
- An icon that looks like two stacked drives identifies a drive that is mirrored.
- An icon that looks like a cracked drive with a question mark identifies a drive on which errors have occurred. For drives with critical errors, color monitors show a red icon.
- An icon that looks like two stacked drives with a crack through them identifies a mirrored drive on which errors have occurred. For drives with critical errors, color monitors show a red icon.
- A question mark (?) in place of the drive letter indicates the drive is detached.

The remaining fields in the row to the right of the icon describe the drive in more detail:

- The **Drive** column contains the logical drive letter.
- The **Type** column describes the current type of the logical drive.
- The **Status** column describes the current status of the logical drive.
- The **Disks** column describes the location of the logical drive upon the physical drive. The first number represents the physical disk that contains the primary partition. The second number represents the physical disk that contains the secondary partition.
- The **Verified** column describes the last date on which a mirrored drive was either verified by the FTADMIN utility or formatted by the FTSETUP utility. If a drive has not been verified, this column displays `Never verified`.

Error Information

The error information section contains information about disk errors on the selected drive. On color monitors, critical errors are displayed in red. For each error, the following columns of information are shown:

- The **Drive** column contains the drive letter of the logical drive on which the error occurred.
- The **Code** column contains a numerical code that identifies the error.
- The **Severity** column contains a status word that indicates the severity of the error. The possible values for the Severity column in decreasing order of severity are: Critical, Error, and Warning.
- The **Disk Block** column contains a 10-digit number that indicates which disk block had the error.
- The **Date/Time** column indicates the date and time that the error occurred.

Selecting a Server

Use the FTADMIN utility to monitor and correct errors locally and remotely. You can view any of the servers in any domain in which the client is logged on. To monitor and correct errors at a remote server, you must select the remote server.

To select servers in other domains:

1. Open **FTADMIN**.

   Note: You can, instead, start the FTADMIN utility from the command line by entering `FTADMIN` at an OS/2 prompt. To start the FTADMIN utility at a server other than the local server, enter `FTADMIN \\` *`servername`*, where *servername* is the name of the server you want to administer.
2. Select **Options**.
3. Select **Select server**.

   A window is displayed containing a list of the servers in the local domain that are enabled for Fault Tolerance.

   Note: When logging on using User Profile Management, Fault Tolerance performs a domain-wide verification of the user ID. If you log on as a user (not an administrator), the **Select server** field is empty because your domain has no servers that you can administer.
4. Select the server that you want to monitor, or type the server's machine name in the **Set server to** field.
5. Select **Ok** from the Select Server window.
6. If you are prompted to supply a password, type the password in the **Enter password** field, and then select **Enter**. The requested password is a User Profile Management password for the server that is in another domain. The password must be associated with your user ID on that domain.

   The Fault Tolerance Administration main window (Figure 13 on page 184) returns, displaying drive information for the server you specified.

Setting Up to Receive Fault Tolerance Alerts

Use the following procedure to receive alerts.

To receive Fault Tolerance alerts:

1. Make sure the user IDs of those who are to be sent alerts are given administrator privilege.
2. Add these user IDs to the **alertnames** parameter in the IBMLAN.INI file.
3. Make sure the Alerter service is listed in the **srvservices** parameter in the IBMLAN.INI file.
4. Use the FTMONIT utility or the FTADMIN utility to turn on the Fault Tolerance Alerts setting.

For more information, see the following topic:

- "Turning Disk Alerts On and Off"

Turning Disk Alerts On and Off

By default, the FTMONIT utility issues an alert whenever a critical disk error occurs. The administrators who receive alerts are specified by the **alertnames** parameter in the Server section of the IBMLAN.INI file. If the Requester service is not started on a workstation when a disk error occurs, the FTMONIT utility starts the Requester and Alerter services and then sends the alert to the administrators that are set up to receive error alerts.

Three classes of fault tolerance alerts indicate different levels of severity:

- **Warning** alerts inform you that a read or write error occurred and was corrected. No alerts are sent to administrators listed by the **alertnames** parameter, but Fault Tolerance displays an error message. The cracked-drive icon is displayed. The cracked-drive icon is cleared when the user views the error.
- **Error** alerts inform you of more severe disk errors, such as excessive disk failures or verification failures. An alert is sent, and an error message is displayed. The cracked-drive icon is displayed.
- **Critical error** alerts inform you of critical disk errors, such as a complete disk failure or a mirrored drive that has been detached. An alert is sent, and an error message is displayed. The cracked-drive icon is displayed. On color monitors, the error message and drive icon are red.

To see a list of the possible errors reported by Fault Tolerance, view the help index in the FTADMIN utility. The errors are listed under the “logged errors” topic.

To turn alerts on or off:

1. Open **FTADMIN**.
2. Select **Options**.
3. Select **Alerts setting**.
4. To turn disk error alerting on, select the **Send alerts** check box. To cancel disk error alerting, deselect the check box.
5. Select **Ok** in the **Alerts setting** window.

Note: Changes made to disk alerts are not permanent and will not last through a system shutdown.

Viewing Drive Statistics

Drive statistics are available for each drive, whether it is mirrored, duplexed, or neither. These fault monitoring statistics tell you if the drive is mirrored and how many reads and writes, recovered and unrecovered faults, and hotfixed faults have occurred. Statistics are kept from the time the workstation was started or from the last time the statistics were cleared.

To view or clear drive statistics:

1. Open **FTADMIN**.
2. Select the drive for which you want statistics.
3. Select **Drive**.
4. Select **Statistics**.

   The displayed statistics have the following meanings:

   Statistics **Definition**

   Status Indicates whether errors have been detected.

   Primary partition
   Indicates whether the primary partition is enabled. When a drive is enabled, the workstation can perform reads and writes on it.

A disabled drive has critical errors that must be corrected, and it cannot accommodate reads and writes.

Secondary partition
Indicates whether the secondary partition is enabled. This field is shaded if the drive is not mirrored.

Mirror status
Indicates whether the drive is mirrored.

Reads from primary
Indicates the number of successful reads from the primary partition.

Reads from secondary
Indicates the number of successful reads from the secondary partition in a mirrored pair. This field is shaded if the drive is not mirrored.

Writes to primary
Indicates the number of successful writes to the primary partition.

Writes to secondary
Indicates the number of successful writes to the secondary partition in a mirrored pair. This field is shaded if the drive is not mirrored.

Recovered faults
Indicates the number of read faults that were recovered from a mirrored drive.

Unrecovered faults
Indicates the number of faults for which recovery was not possible.

Hotfixed faults
Indicates the number of read or write requests that failed but were hotfixed. The hotfixed faults can have occurred on a drive that was mirrored or on a drive that was not.

5. Select **Clear** to clear statistics.
6. Select **Ok** when you are through viewing drive statistics.

Viewing Information about Logical Drives

The drive information section of the Fault Tolerance Administration main window contains an icon for each of the workstation’s logical drives. Diskette drives, CD-ROM, removable media, and redirected drives are not shown. Several types of icons are used in the drive information section. Refer to “Logical Drive Information” on page 185 for descriptions of the icons.

You can expand the drive information section of the Fault Tolerance Administration main window. The error information section moves to the bottom of the window. The drive information section expands to show detailed information about each drive.

For each logical drive, the following information is displayed:

- Whether or not the drive is mirrored
- The severity of the worst error on the drive (in the **Status** column)
- The physical disks associated with the logical drive

- The time when the drive was last verified

To expand the drive information section:

1. Select **View** from the menu bar of the Fault Tolerance Administration main window.
2. Select **Full drive information**.

   To remove the displayed information, select **Full drive information** again from the View pull-down menu. The **Full drive information** menu choice works like a toggle switch.

Sorting the Error Information

The error information section of the Fault Tolerance Administration main window contains information about disk errors on the selected drive. On color monitors, critical errors are displayed in red. For each error, five columns of information are displayed. Refer to “Error Information” on page 185 for a description of each information column.

The errors listed in the error information section of the Fault Tolerance Administration main window can be ordered by time or by severity.

To sort errors by time of occurrence from oldest to most recent:

1. Open **FTADMIN**.
2. Select **View**.
3. Select **Sort errors by time**.

To sort errors by severity:

1. Select **View** from the menu bar of the Fault Tolerance Administration main window.
2. Select **Sort errors by severity**.

Correcting Disk Errors

Many disk errors that Fault Tolerance detects can be corrected. As part of fault recovery, Fault Tolerance displays a prompt informing you about the type of error detected and provides information about the best way to correct the error.

For purposes of fault recovery, four types of error are monitored:

- Self-correcting errors
- Administrator-corrected errors using the FTADMIN utility
- Repeated drive failures
- Complete hard-disk failures

During error correction, you can correct individual errors, all errors on a drive, or all errors on all drives. Some errors are self-correcting and do not require your intervention. More serious errors require that you perform an action as part of the error correction.

Online helps are available for each error. For a list of errors and corresponding corrective actions for disk errors found by Fault Tolerance, see the FTADMIN help.

You can use several methods to correct errors found by Fault Tolerance.

To correct errors:

1. Open **FTADMIN**.
2. Select the error or drive on which you want to perform error correction.
3. Select **Error**.
4. Select one of the following items:
   - If you want to correct a specific error, select **Correct**.
   - If you want to correct all errors on a specific drive, select **Correct all on selected drive**.
   - If you want to correct all errors on all drives on the server, select **Correct all**.

   Note: Using the mouse to double-click on an error message in the Fault Tolerance Administration main window has the same effect as selecting that error and selecting **Correct** from the Error pull-down menu. Double-clicking on a drive icon in the drive information section of the Fault Tolerance Administration main window has the same effect as selecting that drive and selecting **Correct all on selected drive** from the Fault Tolerance Administration main window.
5. When correcting multiple errors, select **Yes** in the confirmation window that pops up to confirm and correct one error at a time. To correct all errors automatically, select **No**.

   If you select **Yes**, a message window is displayed, describing each error and the corrective action to be taken.

   If you select **No**, the FTADMIN utility attempts to correct the selected errors automatically on the selected drive. If any errors cannot be automatically corrected, the uncorrected errors are listed in the error information section of the Fault Tolerance Administration main window. To correct the remaining errors, correct each error individually, or correct all errors and, when prompted with the message `Do you want to confirm each corrective action before it is taken?`, select **Yes**. A message window is displayed describing each error and the corrective action to be taken.

For more information, see the following topics:

- “Automatically Corrected Errors”
- “Correcting Cracked Mirrored Drives” on page 191
- “Repeated Disk Failures” on page 191

Automatically Corrected Errors

Disks can develop bad disk sectors in the course of normal workstation operation. In most instances, these errors are self-correcting, and HPFS fixes them without losing or damaging data. A message in the error information window informs you of the error, but no alert is sent.

If errors are detected on a disk during system startup, the FTMONIT utility attempts to verify or compare all sectors on both the primary and secondary partitions of mirrored drives. Any inconsistencies are corrected, and a message is displayed indicating which drive is being verified. If the drive is in use when the FTMONIT utility tries to verify it, the verify operation does not work. You must use the FTADMIN utility to verify the drive manually.

Correcting Cracked Mirrored Drives

When drives in a mirrored pair have had a disk error, the drive is called a *cracked mirror*. The drive icon on the FTADMIN utility main window appears cracked, and Fault Tolerance sends an error alert. Actions such as turning off the workstation without running Shutdown can cause cracked mirrors.

If the cracked mirror was caused by a disk error, correcting the error usually clears the cracked mirror. Refer to “Correcting Disk Errors” on page 189 for more information. In some cases, especially those involving mechanical or electronic damage to a hard disk or its controller, the error cannot be corrected by Fault Tolerance. Fault Tolerance preserves the data, but you must still intervene. In these cases, you must back up the drive, reformat it, and restore it, or in the worst cases, replace a drive controller or hard disk.

Repeated Disk Failures

Repeated failures can indicate that a hard disk is going to fail completely. Fault Tolerance sends an error alert when a disk’s failure rate is excessive.

Excessive failures can indicate that the disk should be reformatted or replaced. When you get an excessive-failure alert, make a backup copy of all drives that have a primary or secondary partition on the failing disk. Next, run the diagnostics for the hard disk (supplied by the disk manufacturer) to determine whether the disk needs reformatting.

If the diagnostics require a low-level format of the disk, the reformatting removes all partitions on that disk. If a secondary partition is destroyed, the system marks the primary partition as unmirrored. If the primary partition is destroyed, leaving just the secondary partition (a detached partition), the secondary partition is represented by a question mark (?) as the drive letter.

You can recover the detached partition, making it visible to the operating system (see “Recovering a Detached Secondary Partition” on page 182).

Note: If excessive errors occur on SCSI drives or your system hangs, make sure the SCSI adapters are terminated properly. Refer to the documentation that came with the adapters for more information.

Verifying Drives

Verification consists of reading all the used sectors (sectors that contain either data or controls) on both the primary and secondary partitions of a mirrored drive and comparing the data. If an inconsistency is found between the data on the two partitions, the data on the partition with the error is replaced with the data from the partition without the error. Any drive that is represented by a double-drive icon (mirrored) can be verified.

Disk errors and loss of power can cause the data on the primary partition to no longer match the data on the secondary partition. Verify drives when you restart a workstation after a power interruption (if the Uninterruptible Power Supply service is not in effect) but not before first correcting all errors on the drive.

To verify a single mirrored drive:

1. Open **FTADMIN**.

2. Highlight the drive you want to verify.
3. Select **Drive**.
4. Select **Verify**.

To verify all mirrored drives on the server:

1. Select **Drive**.
2. Select **Verify all**.

Running the FTADMIN Utility Remotely

You can run the FTADMIN utility from a workstation outside of the domain on which Fault Tolerance is active. It can also be run remotely as a public application. Several prerequisites must be satisfied for you to do this:

- The FTADMIN utility must either be installed on the remote workstation itself or be properly defined as a public application on the network to be administered. To use the FTADMIN utility from a workstation on which it is not currently installed, the proper aliases must also be defined for it, and the appropriate access controls must be in place.
- You mut copy the following files from the server to the remote workstation:
  - IBMLAN\NETPROG\FTMONIT.EXE
  - IBMLAN\NETPROG\FTADMIN.HLP
  - IBMLAN\NETPROG\FT.DLL
- You must be logged on to the network as an administrator.

If the previous prerequisites are satisfied, type

```
FTADMIN \\servername
```

on the command line, where *servername* is the name of the server to administer.

Using the FTREMOTE Utility

The FTREMOTE utility is a subset of the FTADMIN utility and the FTSETUP utility that can execute a set of Fault Tolerance commands contained in a command file, similar in concept to an AUTOEXEC.BAT file or a logon script file. Before executing these commands, the FTREMOTE utility can compare a previously recorded drive-details report to the current one and run commands depending on which items on the details reports match.

The FTREMOTE utility can perform many of the common Fault Tolerance tasks that do not require the administrator to be present. The tasks it can perform include:

- Automatically activating Fault Tolerance (if it is not already activated).
- Configuring the drives to use Fault Tolerance in an unattended state.
- Verifying mirrored drives.
- Correcting disk errors.

For information on how to use the FTREMOTE utility, see *Command Reference*.

Fault Tolerance Recovery Procedures

Fault Tolerance should be used on any server that contains vital data or requires high system availability. Mirroring the drives on a hard disk makes it easier to recover from a disk failure because the system keeps two up-to-date versions of the data.

OS/2 Warp Server Fault Tolerance is designed to tolerate, correct, and recover from most recurring faults. Fault Tolerance does not, however, protect a system from the loss of two disks at the same time. If one of the mirrored disks fails completely, manual recovery is required.

The best way to use Fault Tolerance to recover from a total disk failure in a short time frame is to have a recovery plan. Consider the following tips to ensure successful recovery:

- Each time the hardware configuration changes, make a backup of the configuration. This backup may be needed to recover from a failed system partition.
- Install the OS/2 Boot Manager at the beginning of the first hard disk. Then create all the drives as logical drives.
- After all drives are mirrored, copy C:\FTCFG.SYS to the second 386 HPFS startup diskette. Also, run the FTREMOTE utility without parameters, and save the FTSTATUS.LOG file. This file contains a summary of the drive locations and is very helpful during drive recovery.

  Each time the drive configuration is changed, the startup diskette should be updated and the FTREMOTE utility should be rerun.
- Several files are needed when the recovery procedure must be done from diskette. Save a copy of the files listed in “Recovery from Total Failure of a Nonmirrored Disk”.

  Note: Several of these files are DLLs. Make sure the LIBPATH statement in the CONFIG.SYS file on the second diskette references the location of these files during the recovery scenario.

For more information, see the following topics:

- “Recovery from Total Failure of a Nonmirrored Disk”
- “Recovery from Total Failure of a Mirrored Disk” on page 195

Recovery from Total Failure of a Nonmirrored Disk

This procedure describes how to recover from a failed disk that is not mirrored. You need a drive map that shows the partitions, logical drives, and the size in megabytes of each. One way to generate a drive map is to run FTREMOTE to generate a status file that lists the current configuration. For more information, see *Command Reference*.

To recover from a total failure of a nonmirrored disk:

1. Start with the following configuration. The prime character (') indicates a secondary partition. D: is the primary partition on Disk 1, and the secondary partition is D:’ on Disk 2, and so on.

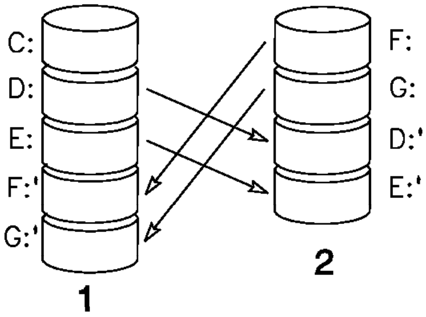


Figure 14. Fault Tolerance Current Drive Configuration

2. Because Disk 1 has failed, replace the hard disk.

   Note: If the disk that failed has a system partition, you must install the system partition from your reference diskette.
3. Perform the following steps only if the failed disk contains the startup drive:
   a. Install the operating system. If you plan to mirror the C drive, it must be formatted for HPFS. Otherwise, formatting the C drive as HPFS is recommended but not required.
   b. Install OS/2 Warp Server with the Fault Tolerance Support option.

   At this point in the procedure, the two detached secondary partitions are denoted by a question mark (?).

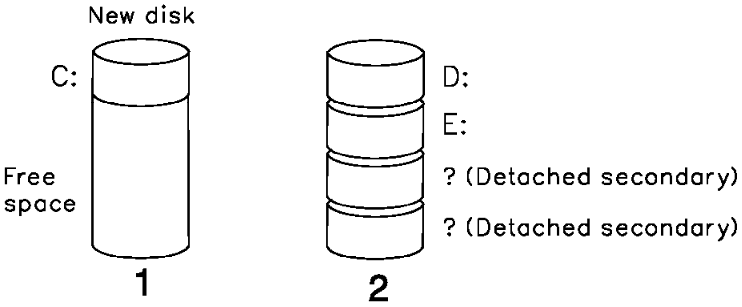


Figure 15. Fault Tolerance Changed Drive Configuration

4. Run the FTSETUP utility, and using your drive map, recover the detached secondary partitions and remirror the drives. For this example:
   a. Recover the first detached secondary drive as a secondary of a mirror and assign it drive letter D:
   b. Recover the second detached secondary drive as a secondary of a mirror and assign it drive letter E:
   c. Mirror drive F. (This disk becomes F:' on Disk 1.)
   d. Mirror drive G. (This disk becomes G:' on Disk 1.)
5. Save the changes, run Shutdown from the desktop, and restart the system. The system is now restored, and the drive letters are restored to the values they had prior to disk failure.

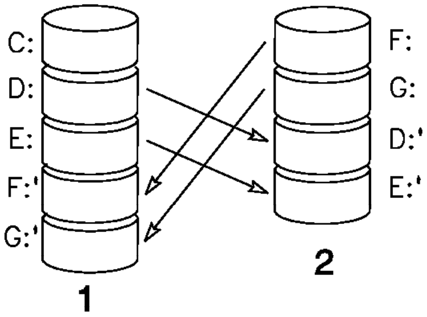


Figure 16. Fault Tolerance Restored Drive Configuration

Recovery from Total Failure of a Mirrored Disk

This procedure describes how to recover from a failed disk that is mirrored. In this example, the first disk has failed and must be replaced. The computer used in this example consists of a Personal System/2 (PS/2) model 95 with two 400MB SCSI hard disks, one SCSI controller, and a 1.44MB floppy disk drive. The OS/2 operating system, OS/2 Warp Server, 386 HPFS, and Fault Tolerance are installed on the system.

The OS/2 Boot Manager is installed on the first disk, and all drives are logical drives. The first disk is partitioned as follows:

- Boot manager partition
- Logical drive C, OS/2, mirrored
- Logical drive D, OS/2 Warp Server with 386 HPFS, mirrored
- Logical drive E, data area, mirrored
- Hidden system partition

To recover from a total failure of a mirrored disk:

1. Replace the crashed disk with a new one.
2. Turn on the system with the backup reference diskette of the system partition.
3. Run the automatic configuration, if necessary, and restart the system.
4. Restore the system partition to the new disk.
5. Start from the 386 HPFS diskettes.
6. Install Boot Manager on the new disk.
7. Copy the DLLs (described below) to a valid partition.
8. Create the response file for the FTREMOTE utility. Have the right location information ready in the FTREMOTE response file. This can be determined by the saved FTSTATUS.LOG file. In this example, the response file contains:

```
COMMANDS
<
 RECOVER LOC=2:1 SECONDARY
 RECOVER LOC=2:100 SECONDARY
 RECOVER LOC=2:250 SECONDARY
>
```

9. Run the FTREMOTE utility to recover the partitions.
10. Run LVM to add the new startup drive to the Boot Manager menu.
11. Restart the server.
12. Run the FTADMIN utility to verify and synchronize the other partitions.

Below are the different DLL modules and their locations:

Location	**Module**
\OS2\DLL	• NAMEPIPES.DLL
\MUGLIB\DLL	• NETAPI.DLL
	• NETOEM.DLL
	• NETSPOOL.DLL
	• MAILSLOT.DLL
\IBMLAN\NETPROG	• FTREMOTE.EXE
	• FTR.MSG
\IBMLAN\NETLIB	• FT.DLL
\OS2	• LVM.EXE
	• LVM.DLL
	• LVM.MSG

Chapter 15. Replicating Files

OS/2 Warp Server or LAN Server provides two file replication services—Replicator and DCDB Replicator—that allow a centralized set of files to be selectively replicated from a server to one or more servers or clients.

The Replicator service makes sure that any updates to replicated files are sent in a timely way to all workstations that maintain replicas of the centrally managed information. The Replicator service can replicate up to 1000 entries within a directory or subdirectory. Included in the 1000-file limit is an internal file (*.RP$) that is used by the Replicator service. The depth or path name of any directory cannot exceed 32 subdirectories.

Replication simplifies the updating and coordinating of servers. For example, if you must edit a file on several servers every week, you can update the file on one server and let replication handle the other servers.

You can also use replication to maintain backup copies of files and directories on different workstations, including the domain controller database (although you should use the DCDB Replicator for this, as it is already optimized and set up for this purpose). This way, files lost or damaged on one server can be recovered from another.

The DCDB Replicator service is a subset of the full Replicator service, optimized for the replication of the domain controller database. Many of the parameters that must be set to back up the DCDB using the full Replicator service are preset in the DCDB Replicator service. Both services can run simultaneously without conflict. For more information on DCDBREPL, see "Using the DCDB Replicator Service to Back Up the DCDB" on page 21.

You can use the Replicator service to replicate administrative or application information, including configuration profiles and application directories. The Replicator service provides:

- Replication of one or more directories from any server to any set of servers or clients
- Selective replication, allowing each importer to replicate only the directories appropriate to it
- Ability to add to or delete from the set of directories being replicated dynamically
- Ability to replicate only files in a first-level directory or the entire tree, including all files and subdirectories
- Directory-level integrity checking to make sure that partial replication of a directory never occurs
- Ability to replicate information locally to provide a local mirroring service

The server sending the data is called the *exporter*. clients and servers receiving the data are called the *importers*.

Each exporter stores all such information under one common path, called the *export path*. The location of this path can be configured on each exporter. The importer workstation for any replication operation uses a single path, called the *import path*, as the target of all copied directories.

Before you can replicate files across a domain, you must prepare the computers that will be sending (exporting) files, and the computers that will be receiving (importing) files. Follow the steps in “Setting Up The Exporter” and “Setting Up the Importer” on page 201 to replicate files.

The export path must contain a set of subdirectories. The objects copied are files in each subdirectory. To add data to be replicated, put it in a subdirectory of a server’s export path. To stop sending updates, delete the directory from the export path. To initiate receiving copies of a given directory, create an empty directory of that name under the import path in the intended path at the intended importer. To stop receiving updates, delete the directory from the import path.

Exporters check for changes to their directories at the interval you have set and notify importers of any changes that occurred during that interval. Importers then perform the specified file replication. Importers never check an exporter for changes unless they get an update notice. A *pulse* mechanism guards against lost update notices by retransmitting the last message at a regular interval when no new messages are generated. Sequence numbers in each message allow importers to identify lost notices or repeats of notices they have already seen.

Change notices tell an importer which directory to check for changes. The importer must determine what has changed. To avoid overloading the exporter with update efforts following a change notice, the importer accesses the changed directory at random intervals.

For more information on the Replicator and DCDB Replicator service parameters, refer to *Performance Tuning*.

For more information, see the following topics:

- “Setting Up The Exporter”
- “Setting Up the Importer” on page 201
- “Using the Replicator Service” on page 202
- “Example Configuration” on page 203

Setting Up The Exporter

Only servers can export files. The following steps show how to set up a server to replicate files for the first time.

To set up a server as an exporter:

1. Use a text editor to create an ASCII-format REPL.INI file in each first-level directory of the export path. REPL.INI lets you control how files and subdirectories in that first-level directory are replicated. The REPL.INI file is read by the Replicator service when one of the following occurs:
   - The Replicator service is started using NET START REPLICATOR from the OS/2 command prompt.
   - The Replicator service is started from the command line or LAN Server Administration.
   - The Replicator service is automatically started when the server starts.
   - A new first-level directory is created.

The REPL.INI file contains only two parameters: **extent** and **integrity**. Each parameter has two possible values: `TREE` and `FILE`.

Create a REPL.INI file containing an **extent** and **integrity** statement in each first-level directory you want to replicate in the exporting tree. To prevent a first-level directory from being replicated, do not create a REPL.INI file in the directory. Use one of the four possible REPL.INI files illustrated below.

a. To replicate files and subdirectories sending updates file-by-file as changes occur when the file has been stable for a specified period, create the following REPL.INI file:

```
extent = tree  integrity
= file
```

b. To replicate files and subdirectories sending updates when the tree has been stable for a specified period, create the following REPL.INI file:

```
extent = tree  integrity = tree
```

c. To replicate only files sending updates file-by-file as changes occur when the file has been stable for a specified period create the following REPL.INI file:

```
extent = files  integrity = file
```

d. To replicate only files sending updates when the tree has been stable for a specified period, create the following REPL.INI file:

```
extent = files  integrity = tree
```

The following list describes each REPL.INI parameter:

extent
Specifies whether all subdirectories of this first-level directory should be replicated.

If the value is `TREE`, all files and subdirectories in the first-level directory are replicated. If the value is `FILE`, all files in the first-level directory are replicated but not any of its subdirectories.

Default value: TREE

integrity
Specifies the type of updates sent from the exporter to the importers.

If the value is `TREE`, all files and subdirectories in the first-level directory must be stable for a predetermined interval before any can be replicated. This interval is specified by the **guardtime** parameter in the Replicator section of the IBMLAN.INI file. If the value is `TREE`, it is not possible to replicate to the current directory of an active process on the importer.

If the value is `FILE`, updates are replicated file by file. If the **integrity** parameter value is `FILE`, the **guardtime** parameter has no effect.

Default value: FILE

2. Create a user ID and password for the importer if it is a server or if it is in another domain. Use an ID that is different than the machine name. The importer requires a user ID for the following reasons:

- When a client is an importer, it logs on to replicate using its machine name defined as a system ID to the domain controller when the client was installed.

- When a server is an importer, it cannot log on to replicate using its machine name because it periodically changes its system password.
- When an importer is in another domain, the machine name is not defined as a system ID in the exporting domain.

3. Edit replicator parameters in IBMLAN.INI. Refer to “Parameters Descriptions - Replicator Section” in *Performance Tuning* for more information.

   Use the values in one of the following conditions to set up replication at the exporter:

   a. If exporting to an importer in the same domain, set values for parameters as follows:
      - replicate=export
      - exportpath=absolute path to the exporting trees
      - exportlist=importer receiving updates
      - add REPLICATOR to srvservices section.

   b. If exporting to more than one importer in the same domain, set values for parameters as follows:
      - replicate=export
      - exportpath=absolute path to the exporting trees
      - exportlist=importer1;importer2 receiving updates
      - add REPLICATOR to srvservices section.

   c. If exporting to an importer in another domain, set the values for parameters as follows:
      - replicate=export
      - exportpath=absolute path to the exporting trees
      - exportlist=importer1;domain receiving updates
      - add REPLICATOR to srvservices section.

   d. If exporting to more than one importer in another domain, set values for the parameters as follows:
      - replicate=export
      - exportpath=absolute path to the exporting trees
      - exportlist=importer1;importer2;domain receiving updates
      - add REPLICATOR to srvservices section.

   e. If exporting and importing on the same computer, set values for parameters as follows:
      - replicate=both
      - exportpath=absolute path to the exporting trees
      - importpath=absolute path to the importing tree
      - logon=importer’s logon ID
      - password=importer’s logon PW
      - add REPLICATOR to srvservices section.

      Use any or all of the following conditions to tune the performance of the exporter.

   f. To change how long the tree must be stable before replication occurs when the **integrity** is set to **tree** in REPL.INI, set values for parameters as follows:
      - guardtime=0-interval/2

   g. To change how often, in minutes, subdirectories and files in the export path are checked for changes, set values for parameters as follows:

  - interval=1-60

  h. To change how often the exporter sends extra updates, besides those sent when a change occurs in the export path, set values for parameters as follows:

     - pulse=1-10 (This is multiplied times the interval to determine how often redundant updates are sent.)

  i. To change how often connections are distributed to importers, set values for parameters as follows:

     - random=1-120 (seconds)

4. Give the importer access to the export path. To receive updates, an importer must be given both read (R) and attributes (A) access permissions to the files in the export directories.

   a. Create an access profile for the export path. See “Creating Access Control Profiles for Resources without Aliases” on page 92.

   b. Assign read an attributes permissions to user or group IDs who are to receive replicated files.

   c. Apply the access profile to the directories in the export path. For information on the Apply function, see “Propagating Access Control Profiles to Subdirectories” on page 88.

5. Start the Replicator service from the OS/2 command line by typing:

   ```
   NET START REPLICATOR
   ```

Setting Up the Importer

Servers or clients can import files. Following are the steps for setting up a computer to import files for the first time.

To set up a server as an importer:

1. Create the import directory tree structure by creating a directory for all first-level directories being imported. There can be only one import path regardless of the number of exporters and exporting trees. So, to receive updates from the exporters, all first-level subdirectories must be in the import path. It is not necessary to create subdirectories below the first level. They are created by the Replicator service at the time of replication.
2. Create a user ID and password if the importer is in another domain. Use an ID that is different than the machine name if the importer is a server. The ID will need to be defined to both the exporting and the importing domain controllers.
3. Edit replicator parameters in IBMLAN.INI. Refer to *Performance Tuning* for more information.

   Use values in one of the following conditions to set up replication at the importer.

   a. If importing from an exporter in the same domain, set values for parameters as follows:

      - replicate=import
      - importpath=absolute path to the importing tree
      - importlist=exporter sending updates
      - tryuser=yes
      - add REPLICATOR to wrkservices section.

   b. If importing from more than one exporter in the same domain, set values for parameters as follows:

    - replicate=import
    - importpath=absolute path to the importing tree
    - importlist=exporter1;exporter2 sending updates
    - tryuser=yes
    - add REPLICATOR to wrkservices section.
   c. If importing from an exporter in another domain, set values for parameters as follows:
      - replicate=import
      - importpath=absolute path to the importing tree
      - importlist=exporter1;domain sending updates
      - tryuser=yes
      - add REPLICATOR to wrkservices section.
   d. If importing from more than one exporter in another domain, set values for parameters as follows:
      - replicate=import
      - importpath=absolute path to the importing tree
      - importlist=exporter1;exporter2;domain sending updates
      - tryuser=yes
      - add REPLICATOR to wrkservices section.

      Add one or both of the following alternatives to one of the preceding conditions.
   e. If the importer is a server, add the following replicator parameters to one of the other importer conditions above:
      - logon=importer's logon ID
      - password=importer's logon PW
   f. To prevent replication while a user is logged on, set **tryuser** to no. Replication does not occur as long as a user is logged on.
4. Start the Replicator service by typing at the OS/2 command line:
   ```
   NET START REPLICATOR
   ```

Using the Replicator Service

Use the following procedure to complete the replication of files.

To replicate files:

1. Users on importers should not change files in the import path. Such changes are lost as soon as the Replicator service sends updates to the importer.
2. Force the immediate replication of files by issuing commands at both the exporter and importer to stop and start the Replicator service.
   a. Stop the Replicator service if it is running by typing NET STOP REPLICATOR at an OS/2 command line.
   b. Start the Replicator service by typing NET START REPLICATOR at an OS/2 command line.
3. Prevent replication of files and subdirectories in a first-level directory by creating a USERLOCK. *xxx* file. The USERLOCK. *xxx* file can be empty. The file extension *xxx* can be any extension. The file name USERLOCK. *xxx* acts as a signal to the Replicator service. While USERLOCK. *xxx* exists, replication in that directory is prevented. When USERLOCK. *xxx* is deleted, replication restarts.

USERLOCK. *xxx* supplements the **guardtime** parameter by letting you decide when files are ready for replication. Refer to “Parameter Descriptions - Replicator Section” in *Performance Tuning*.

Note: USERLOCK. *xxx* works only in a first-level subdirectory beyond the export path, and only if **integrity=**`TREE`.

4. Verify that replication is occurring by checking for the existence of a signal file in the import path. The Replicator service puts a *signal file* in each first-level subdirectory of an import directory. Signal files indicate the status of the directory and are named differently according to their meanings.

Signal File **Meaning**

OK.RP$ The directory is receiving updates from the exporter.

NO_MASTR.RP$
The directory is not currently receiving updates from an exporter for one of the following reasons:
- The server exporting this directory is not operating.
- Something is wrong with the replication setup.
- The exporter has stopped exporting this directory. (The directory may no longer be in the export path, or the REPL.INI file has been removed from the directory.)

NO_SYNC.RP$
The directory is receiving updates, but they may not be current. Use the NET ERROR command to view the error log for more information. The cause can be one of the following:
- A communication failure
- A system failure on the exporter
- Incorrect access permission to the export path
- Open files on the importer or exporter

5. Determine the last time replication occurred by checking the time stamp on the OK.RP$ file in the import path.
6. Clean up a replicated tree at the importers by deleting the first-level directory from the import path. Removing this directory deletes the data at the importer and prevents future replication.
7. Stop all replication by stopping the Replicator service at one or both computers and removing Replicator service from the IBMLAN.INI files. If you leave Replicator in the IBMLAN.INI files, the service starts automatically the next time you start the client and Server services at the exporter and importer.

Example Configuration

The following presents an example configuration for using the Replicator service. Workstation IMP1 is set up as an importer to maintain replicated files for the server workstations EXP1 and EXP2. The importers and exporters are in the same domain.

The server workstation EXP1 is configured with the following IBMLAN.INI parameter entries in the Replicator section:

```
replicate = export
exportlist = IMP1
exportpath = C:\EXPORT
```

The Replicator service is added to the srvservices section in the IBMLAN.INI file. The export directory structure of EXP1 is shown in the following figure.

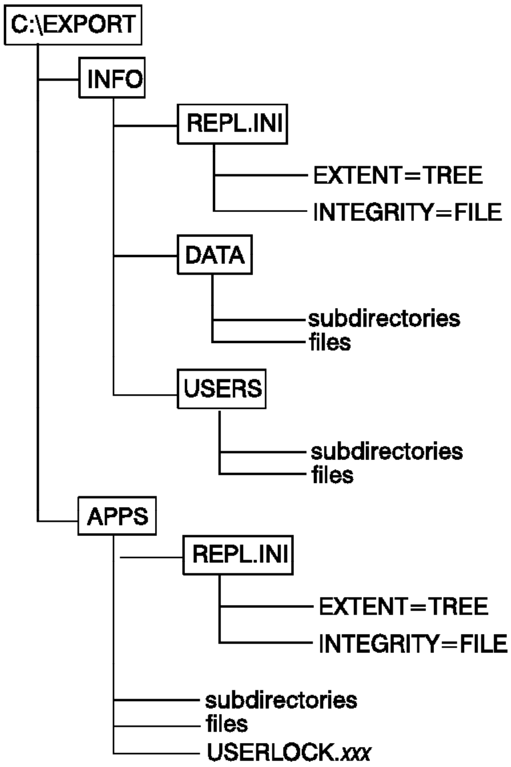


Figure 17. Exporter EXP1 Directory Structure

The server workstation EXP2 is configured with the following IBMLAN.INI parameter entries:

```
replicate = export
exportlist = IMP1
exportpath = D:\REPL
```

The Replicator service is added to the srvservices section in the IBMLAN.INI file. The export directory structure of EXP2 is shown in the following figure.

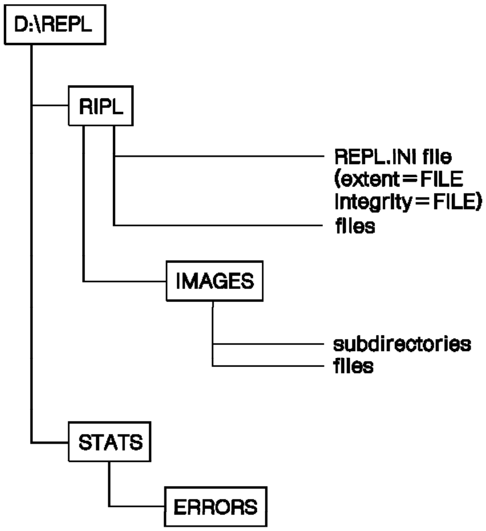


Figure 18. Exporter EXP2 Directory Structure

The workstation IMP1 is set up as the importer with the following IBMLAN.INI parameter entries in the Replicator section:

```
replicate = import
importlist = EXP1;EXP2
importpath = C:\BACKUP
tryuser = yes
```

The directory structure of IMP1 is shown in the following figure.

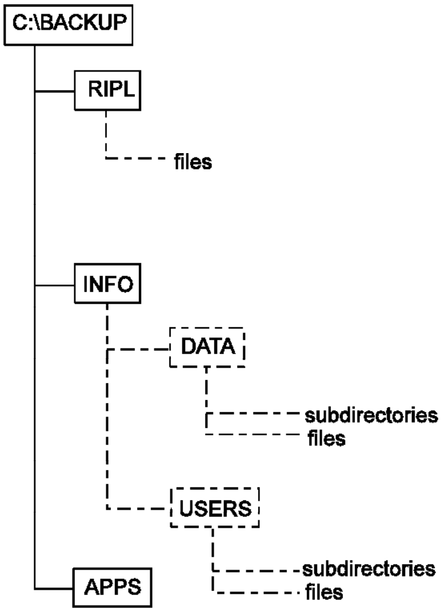


Figure 19. Importer IMP1 Directory Structure

First-level directories must be created manually on IMP1 to indicate which of the exporter directories are to be replicated. The remaining directory structure and its contents (subdirectories and files) are created by the Replicator service.

The REPL.INI file in D:\REPL\RIPL of EXP2 allows only the files of the IMAGES subdirectory to be replicated. Its subdirectories are not replicated. Nothing in the \APPS subdirectory is replicated because of the USERLOCK. *xxx* file in the export directory. All subdirectories and files are replicated in the INFO directory.

Setting the **tryuser** parameter to YES in the IBMLAN.INI file in IMP1 allows replication to occur when a user with the proper access permissions is logged on. IMP1 is also defined as a user ID with access to the export paths of EXP1 and EXP2 so that replication can occur even when no user is logged on. The use of the importer’s user ID is possible only if IMP1 is a client. When the server changes its password, the replication does not work using the machine name unless the password is kept current at the exporters.

Chapter 16. Installing and Configuring Remote IPL

Remote initial program load (remote IPL) is the process of downloading IPL files from a server to a workstation in order to start the workstation.

Use remote IPL to start medialess workstations (workstations without disk drives) and workstations that do not have OS/2 LAN Requester or DOS LAN Services installed.

The following clients are supported by the Remote IPL service:

- OS/2 Warp 3.0
- OS/2 Warp 4.0
- WorkSpace On-Demand 1.0
- WorkSpace On-Demand 2.0
- DOS

Note: In order to use **LAN Server Administration**, OS/2 Warp 3.0 clients need OS/2 Warp 3.0 FixPak 32 or later, and OS/2 Warp 4.0 clients need OS/2 Warp 4.0 FixPak 6 or later.

Workstations loaded by remote IPL are called *remote IPL workstations* (also referred to as remote IPL clients). Remote IPL workstations can be started from IPL files on a server. When the workstation is started, the designated server sends IPL files to the workstation.

OS/2 Warp Server supports 802.2 RIPL using NetBIOS as the network protocol, and Dynamic Host Communication Protocol (DHCP) boot using TCP/IP as the network protocol. DHCP boot requires the Preboot Execution Environment (PXE) extensions as defined in the Intel Wired for Management specification. PXE is usually provided on ROM/PROM/EPROM on the network adapter, or on the system board. A client that does not have PXE support must use 802.2 RIPL.

These two boot methods and network protocols can be used in combination to provide the following types of boot clients:

- 802.2 RIPL/NetBEUI
- 802.2 RIPL/TCPBEUI
- DHCP PXE RIPL/TCPBEUI
- DHCP PXE RIPL/NetBEUI

You must configure TCPBEUI on the server in order to run DHCP PXE RIPL/TCPBEUI or 802.2 RIPL/TCPBEUI on a client. You can use LANINST to configure TCPBEUI on the server. For more information about this, see *Quick Beginnings*.

For more information, see the following topics:

- “DHCP Boot” on page 208
- “Remote IPL Control Files” on page 211
- “Installing Remote IPL Using the OS/2 RIPLINST Utility” on page 222

DHCP Boot

DHCP PXE RIPL uses IP, which is a routeable protocol. This protocol allows the client to be on a different subnet than the boot server's subnet. DHCP servers can provide two functions: dynamic IP address assignments and centralized network boot services. In DHCP with PXE, the IP address server can be on a system separate from the boot file server. You can choose to have more boot servers with fewer DHCP servers to assign IP addresses, which increases the scalability of the DHCP server.

The Boot Information Negotiation Layer (BINL) server is configured to identify the IP address of the code server and the path and name of the DHCP boot method's bootstrap loader. A PXE Proxy server services a BINL server when a BINL server service is not running on the same system as the DHCP server. The PXE proxy informs the PXE client of the IP address where the BINL server is located. If the BINL service co-exists with DHCP service on the same system, then the DHCP proxy service is not needed. The DHCP, PXE Proxy, and BINL servers can physically be on separate machines. The Trivial File Transfer Protocol (TFTPD) server must be on the code server.

Note: All servers, except for the PXE Proxy, must be operational for the boot process to complete successfully.

The PXE protocol locates the DHCP server and finds the appropriate boot server to load the DHCP boot method's bootstrap loader. The bootstrap loader locates the <client>.INF file on the code server. Bootstrap loader uses the client's LAN adapter address to determine the name of the <client>.inf file and its location on the server. Bootstrap downloads the <client>.inf file, and then downloads all the files listed in <client>.inf file. The first entry in the <client>.inf file is the client's RIPL workstation record from the RPL.MAP file. One of the files listed in <client>.inf file is the bpcommon file. The bpcommon file includes a list of files that the client needs for the first phase of boot. Bootstrap downloads these files to the client's high RAM. Bootstrap creates an entry in a lookup table for each file it downloads. The entry includes information about each file, such as file size and the address where the file is located in high RAM. Bootstrap then passes control to OS2LDR, which uses a VDISK to manage the files in high RAM. This brings up the operating system, network, and redirected file system. The redirected file system replaces the VDISK and the initialization process continues using the redirected file system using System Message Block (SMB) protocol.

A progress indicator is displayed throughout the boot process. During the first phase of the bootup process, no operating system or font services are available, so error messages are displayed through BIOS functions. Because only the characters supported by machine ROM BIOS (code page 437) can be displayed, the error messages appear in English. See “Appendix D. DHCP RIPL Bootstrap Messages” on page 281 for a list of these error messages and help. When the DHCP boot bootstrap is loaded and executed successfully, a copyright statement is displayed.

DHCP/BINL Server Configurations for DHCP Boot

To remote boot the DHCP PXE clients from a server, you must have DHCP/BINL server services running and available on the network. In Intel's Wired for Management and NetPC, DHCP server services are extended to include DHCP PROXY and BINL services. You can configure these three services in the following combinations:

- DHCP, BINL, code server with TFTP all on the same system. In this configuration, DHCP PROXY is not needed.
- DHCP and BINL on one system, code server with Trivial File Transfer Protocol (TFTP) on a separate machine. In this configuration, DHCP PROXY is not needed.
- DHCP, BINL, and code server all on separate systems. In this configuration, DHCP PROXY must be installed either on a separate machine or on the BINL server or on the code server.

To support WorkSpace On-Demand DHCP PXE RIPL clients, you must configure a DHCP server that supports the PXE extensions, a BINL server, and a TFTP server. The DHCP server installed by WorkSpace On-Demand 2.0 contains the PXE extensions. This section provides examples of the parameters that must be configured for the DHCP and BINL servers. After the DHCP server is configured, the DHCP configuration data is saved in the file named DHCPSD.CFG and stored in the directory identified by the ETC environmental variable. The ETC default directory name is MPTN\ETC.

When the BINL server is not located on the same machine as the DHCP server, additional parameters must be configured to support PXE clients. The following example of the DHCPSD.CFG contains the parameters of DHCP server type. Note that the vendor type of PXE client has been disabled by being commented. The PXE client vendor option must not be defined for a non-PXE DHCP server.

```
# Server mode setup
servertype   dhcp

# Setup to send options to the pxeclient.  Sent in the encapsulated option 43.
# vendor PXEClient
  {
    option 1 1.1.4.5
    option 2 2
    option 3 3
    option 4 4
    option 5 5
  }
```

For the DHCP server to support PXE clients, you must configure the DHCP server type, and the vendor type for the PXE client. These parameters are in addition to the basic DHCP server parameters such as domain name, subnet mask, default router address, and a range of addresses to be assigned to the clients.

The following is an example of the DHCPSD.CFG file for the additional parameters that must be configured to support PXE clients when the BINL server is located on the same machine as the DHCP server. The parameters shown is this example are DHCP server type and PXE client vendor type.

```
# Server mode setup
servertype pxedhcp
# Setup to send options to the pxeclient.  Sent in the encapsulated option 43.
 vendor PXEClient
  {
    option 1 1.1.4.5
    option 2 2
    option 3 3
    option 4 4
    option 5 5
  }
```

The following is a PROXY DHCP server example of the DHCPSD.CFG file for the additional parameters that must be configured to support PXE clients when the BINL server is not located on the same machine as the DHCP server. The parameters shown is this example are DHCP server type, location of the BINL server, and the PXE client vendor type.

```
# Server mode setup
imageserver 9.3.162.196
servertype pxeproxy

# Setup to send options to the pxeclient.  Sent in the encapsulated option 43.
 vendor PXEClient
  {
    option 1 1.1.4.5
    option 2 2
    option 3 3
    option 4 4
    option 5 5
  }
```

To configure the BINL server, you must define the DHCP boot file name (bpname) and the TFTP server address to the BINL server. After the BINL server is configured, the BINL configuration data is saved in the file named BINLSD.CFG and stored in the directory identified by the ETC environmental variable. The ETC default directory name is MPTN\ETC.

The following is an example of the bpname and TFTP server address that is saved in the BINLSD.CFG file after the BINL server configuration is complete. The bpname must always be \DOS\DHCPBOOT\RPLBOOTP.SYS. In this example, the TFTP server address is 9.3.162.194.

```
# Global Options
# default TFTP server
tftp   9.3.162.194
# Fully qualified boot Image pathname
bpname \DOS\DHCPBOOT\RPLBOOTP.SYS

# SA 0, NIT 1 specific options
sa 0 nit 1
{
  tftp 9.3.162.194
  bpname \DOS\DHCPBOOT\RPLBOOTP.SYS
}
```

The TFTP server does not require any configuration. The TFTP server must be started on the machine that contains the server directory with the location of the \IBMLAN\RPL directory as the base TFTP directory. The following examples show how to start the TFTP server with this directory as the default base directory:

```
Start TFTP Server Example 1:
C:
CD \IBMLAN\RPL
TFTPD
```

```
Start TFTP Server Example 2:
TFTPD C:\IBMLAN\RPL
```

To support frequent remote booting of clients, the default TCP/IP keepalive timer value should be set to 20 seconds.

You can add the configuration files to your startup command file to start DHCP Boot server services. A sample STARTBB2.CMD is below:

```
c:
dhcpsd
binlsd
cd ibmlan\rpl
tftpd
inetcfg -s keepalive 20
```

Remote IPL Control Files

The remote IPL process is controlled by the following files:

- DHCP boot files:
  - <client>.INF
  - bpcommon.ISA, or bpcommon.MCA
  - rfcnames.lst
  - rfcbcst.lst
- .CNF boot block definition file (only 802.2 RIPL)
- RPL.MAP
- File Index Table (FIT)
- NDISDD.PRO

Each server contains only one RPL.MAP, NDISDD.PRO file, and bpcommon file. The bpcommon.ISA file is used to remote IPL DHCP Boot clients on non-Micro Channel machines. The two Micro Channel machine classes use bpcommon.MCA. There are multiple .CNF and FIT files on the server.

The remote IPL service provides default RPL.MAP records, FIT files, CONFIG.SYS, bpcommon, NDISDD.PRO, and DOS image definition files to use when setting up remote IPL requesters. The default files are always used when defining a remote IPL client. If these files do not meet your requirements, you can customize your remote IPL requesters by altering the default files provided.

For more information, see the following topics:

- "DHCP Boot Files" on page 212
- "Boot Block Definition (.CNF) File" on page 213
- "RPL.MAP Control File" on page 215
- "File Index Table (FIT)" on page 218
- "NDISDD.PRO Control File" on page 221

DHCP Boot Files

The DHCP boot files that you might need to update are:

- <client>.INF, where client is the last 8 digits of the LAN address.
- bpcommon.ISA, bpcommon.MCA
- rfcnames.lst
- rfcbcst.lst

When you create a DHCP boot client, the path and file name for that client is created in a mac address subdirectory of /MACHINES, using the first 4 digits of the LAN address:

```
 /MACHINES/MACADDR/client_address
     where client_address is the first 4 digits of the LAN address
```

A client-specific information file is created, using the remaining 8 digits of the LAN address. Below is an example of a US version of a <client>.INF file in the MACADDR subdirectory:

```
0004acec2e6e BJ100 ˜ Fits\BJ100 BB2SVR Z ˜ ˜ ˜ ,,, ˜ R_BB2_cc_DHCPBOOT
\bb20.us\rplbootp.msg
\bb20.us\bpcommon.isa
\fits\BJ100.FIT
\machines\bj100\ibmcom\macs\ibmtrp.os2
\machines\bj100\ibmcom\a1.msg
\machines\bj100\ibmcom\a1h.msg
\machines\bj100\config.sys
\machines\bj100\ibmlan\ibmlan.ini
\machines\bj100\ibmcom\protocol.ini
\machines\bj100\mptn\bin\setup.cmd
\machines\bj100\mptn\etc\dhcpcd.chf
\machines\bj100\mptn\etc\services
```

The first line in the .INF file is client-specific configuration information, including the LAN address. This line is the same as the workstation record entry for this client in the RPL.MAP file. In the example, the LAN address is 0004acec2e6e. The directory structure and filename for this client would be /MACHINES/MACADDR/0004/acec2e6e.INF.

The <client>.INF file contains the path and file name for the common descriptor file bpcommon. When you add a base device, you must add a line to the bpcommon file identifying the path to that device. You will also need to update the client's CONFIG.SYS file for the additional base device.

Two bpcommon files are located in the BB20.cc\IBMLAN\NETPROG subdirectory. The two Micro Channel machine classes use bpcommon.MCA for vga machine classes and bpcommon.MCX for xvga machine classes. All non-Micro Channel machine classes use bpcommon.ISA.

Below is a sample of entries as they would appear in a bpcommon file:

```
\bb20.cc\os2\keyboard.dcp
\bb20.cc\os2\system\country.sys
\bb20.cc\os2\boot\screen01.sys
\bb20.cc\os2\boot\kbdbase.sys
\bb20.cc\ibmcomprotocol\netbeui.os2
\bb20.cc\ibmlan\netprog\netwksta.200
```

The bpcommon and <client>.INF files have list files that are needed for the first phase of the client’s boot process. Rfcnames.lst and rfcbcst.lst are TCPBEUI config files.

When you create a DHCP Boot requester using the LAN Server Administration GUI, the server’s NetBIOS name and its IP address are added to the rfcnames.lst and rfcbcst.lst files. In the PROTOCOL.INI configuration file, the keyword NAMESFILE value is set to a non-zero number. For broadcast node types, if you want the requester to be able to access other servers, you must update the rfcnames.lst and rfcbcst.lst files.

Boot Block Definition (.CNF) File

Boot block definition files define an operating system and the way it is loaded into a remote IPL workstation. Every server record in the RPL.MAP file must contain a reference to a boot block .CNF file. One server record in the RPL.MAP file supports the DHCP boot method for the server, pointing to a dummy .CNF file. DHCP boot does not access this file.

A default .CNF file is provided for all supported network adapters. You do not need to change boot block .CNF files unless it is necessary to have the 802.2 RIPL requester operate with different network drivers.

The following example shows the default WorkSpace On-Demand .CNF file for the IBM Token-Ring that is provided with the 802.2 RIPL service of LAN Server.

```
; OS\2 Boot Block Configuration
; (IBM Token-ring Compatible Adapter)
RPL DOS\RPLBOOT.SYS
DAT DOS\MFSD30.SYS
ORG 1000H
LDR BB20.US\OS2LDR ˜ OS2LDR UFSD.SYS MFSD30.SYS
DAT DOS\UFSD.SYS
DAT DOS\TOKENRING\OS2\PROTOCOL.INI
DAT C:\IBMLAN\DOSLAN\LSP\DXM.MSG
DAT C:\IBMLAN\DOSLAN\LSP\DOS\LT2.MSG
EXE C:\IBMLAN\DOSLAN\LSP\NETBIND.COM ˜ ˜ ˜
;**NETBIOS and IEEE 802.2****************
;DRV C:\IBMLAN\DOSLAN\LSP\DXMT0MOD.SYS PBA=0˜S=12˜C=14˜O=N ˜ ˜
;DRV C:\IBMLAN\DOSLAN\LSP\DXME0MOD.SYS ˜ 10 ˜
;**NETBIOS****************
DRV C:\IBMLAN\DOSLAN\LSP\DXMJOMOD.SYS ˜ 6 ˜
;**NETBIOS****************
DRV C:\IBMLAN\DOSLAN\LSP\DXMAOMOD.SYS 001 ˜ ˜
DRV C:\IBMLAN\DOSLAN\LSP\DOS\IBMTOK.DOS ˜ ˜ ˜
DRV C:\IBMLAN\DOSLAN\LSP\PROTMAN.DOS /I: ˜ ˜
```

Figure 20. WorkSpace On-Demand Boot Block Definition File BB1USNTR.CNF

When dealing with path and directory names, all file name fields either can be fully qualified, or expressed relative to RPLDIR, as specified in the `[Remoteboot]` section in the IBMLAN.INI file:

```
RPLDIR = C:\IBMLAN\RPL
```

If they are fully qualified, the entire path must be specified, including the drive letter and all the subdirectories.

All fields, including .CNF file parameters, are separated by spaces. Some .CNF parameters can contain parameter lists to be used by other software. Fields of these embedded parameter lists must be separated by tilde (˜) characters.

The following table describes .CNF file entry types, along with their expected file names and parameters:

Table 2. Description of the Boot Block Definition.CNF File Entries

Entry	Description
RPL	A .CNF file can contain only one RPL entry. The file name field of this entry specifies the name of the first program to be run on the IPL workstation. No parameters are associated with this file entry.
ORG	A .CNF file can contain only one ORG entry. The second file name field of this entry specifies the hexadecimal segment number of a contiguous memory block on the IPL workstation. Files following this entry in the .CNF file are bound to this memory address. No parameters are associated with this file entry.
DAT	Several DAT entries can be located in a .CNF file. Their file name fields specify data files to be stored in the boot block. These files are not used by RPLBOOT.SYS, but they can be read by DOS Handle I/O functions. No parameters are associated with this file entry.
LDR	LDR applies only to OS/2 and WorkSpace On-Demand workstations. A .CNF file can contain only one LDR entry. The file name field of this entry specifies the name of the loader to use on the IPL workstation. For WorkSpace On-Demand, this entry must include the following file name and parameters: **BB20.US\OS2LDR ˜ OS2LDR OS2KRNL MFSD30.SYS**
EXE	A .CNF file can contain one or more EXE entries. The EXE file name fields specify the names of executable files that are to be used on the IPL workstation. The parameter fields of an EXE entry are passed on to the executable file when it runs.
DRV	A .CNF file can contain one or more DRV entries. The DRV file name fields specify the names of device drivers to be used on the IPL workstation. Each driver entry requires the following parameter fields: • The parameter list for the device driver. Fields of this embedded parameter list must be separated by tilde (˜) characters in the .CNF file. • The additional memory requirements of the device driver, if any, are expressed in decimal kilobytes. • Use the character M if the driver can be moved after initialization. Otherwise, use a tilde (˜) character. Most of the drivers currently available cannot be moved, and the tilde character (˜) should be specified. If the driver can be moved and it requires less memory than the original driver image, RPLBOOT.SYS moves the driver to reclaim the unused memory and adjusts all interrupt vectors that point into that driver memory area. **Note:** The order of field entries must be considered. Place EXE entries before DRV entries. This change allows movable drivers to be placed in memory freed by completed .EXE files. DRV statements are order-dependent. They are processed in reverse order, from last to first.
BASE	BASE applies only to DOS workstations. Only one BASE entry can be in a CNF file. The second field of this entry specifies the hexadecimal segment number (paragraph) that is the boot block base address. The default base address is X'00C0H'.

Note: DHCP boot is controlled by the DHCP PXE/BINL services, not by the Remote IPL service. DHCP boot continues to function even when the remote IPL service has been stopped.

RPL.MAP Control File

The RPL.MAP control file is located in the `\IBMLAN\RPL` directory. The file is updated when you create a requester. The RPL.MAP control file contains records that define the behavior of the remote IPL service for each client. The RPL.MAP control file contains a unique requester record entry for each requester you create. The remote IPL requester definitions in the RPL.MAP control file specify the name of the remote IPL server and the parameters required to IPL that requester. Each requester record has a unique adapter ID field that is used to match the specific machine to that record.

When you use the post-install GETRPL utility, the server records that are enabled depend upon the operating system type. For OS/2 versions 3.0 and 4.0 and WorkSpace On-Demand 1.0, only server records that correspond to LAN adapter types found on the server at that time are enabled. To enable server records for other LAN adapter types, you must update the RPL.MAP file by locating the appropriate server record and removing the semicolon in the first column. For WorkSpace On-Demand 2.0, all token-ring and ethernet server records are enabled if all of the support files needed for the adapter are installed on the server.

RPL.MAP control files consist of two sections. One section describes server records, and the other describes workstation records. Each requester must have a set of server and workstation records residing on the server before 802.2 RIPL can occur. The server records include one line per adapter; the workstation records include one line per workstation.

```
server record fields:
;  1    = yyyyyyyyyyyy
;  2    = boot block configuration file (.cnf)
;  3    = number of retries before default boot
;  4    = time window for retries (in seconds)
;  5    = acknowledge (A,N)
;  6    = loader parameters (~ for os2, image share name for dos)
;  7    = descriptive comment
;  8,9, = ~
;  A    = ,,,
;  B    = ~
;  C    = server record identifier
;  D,E  = ~

; server records
 yyyyyyyyyyyy dosbbntr.cnf 3 10 N IBMLAN$ DOS~TOKEN~RING ~ ~ ,,, Z R_DTK ~ ~
 yyyyyyyyyyyy os240et.cnf 3 10 N ~ OS2~WARP~4.0~IBM~ETHERNET ~ ~ ,,, ~ R_240_OET ~ ~
 yyyyyyyyyyyy bb2us316.cnf 3 10 N ~ WSOD~2.0~3COM~ETHERLINK~16~(3C507) ~ ~ ,,, ~ R_BB20_US_OET316 ~ ~
 yyyyyyyyyyyy bbuntr.cnf 3 10 N ~ WSOD~2.0~IBML~TOKEN~RING~COMPATIBLE~NDIS~ ~,,,~R_BB20_USOTKNTR ~ ~
; workstation record fields:
;  1     = adapter ID (12 hex digits)
;  2     = workstation name
;  3     = ~
;  4     = image file for dos (.img), fit file for OS/2 (.fit)
;  5     = name of rpl server
;  6     = boot drive for OS/2, domain name for DOS
;  7,8,9 = parameters for device drivers 1,2,3
;  A     = additional memory for device drivers 1,2,3. Default: ,,,
;  B     = ~ for OS/2, Z for DOS
;  C     = workstation type; first letter is R -> enabled, D -> disabled
;  D     = ~
;  E     = volume ID string for DOS, IML image file for OS/2
;  F     = P for OS/2 PCNet clients only

; workstation records
100FFFFFFFFF DEFAULT ~ imagefile    RPLSRV1 RPLSRV1DOM ~ ~ ~ ,,, Z ~ R_DTK ~ ~
1000FFFFFFFF DFBB20US ~ FITS\DFBB20US RPLSRV1 Z ~ ~ ~ ,,, ~ R_BB20_US_OTKNTR ~ ~ ~
10005A123456 RPLMACH1 ~ FITS\RPLMACH1 RPLSRV1 Z ~ ~ ~ ,,, ~ R_BB20_US_OTKNTR ~ ~ ~
```

Figure 21. An Example of Server Records and Workstation Records in a RPL.MAP File

The two workstation entries made by the GETRPL utility enable remote IPL services. You may delete these entries if you have defined at least one remote IPL client. If you don't have at least one workstation record or remote IPL client, you should disable the REMOTEBOOT service in your IBMLAN.INI so that the server can be started.

In the RPL.MAP file, DHCP boot method server and client records have a unique field to distinguish them from existing RPL.MAP records. The server record has the following format:

```
yyyyyyyyyyyy BB2ccDHC.CNF 3 10 N ~ Workspace~On-Demand~2~PXE~DHCP~BOOT~FOR~TOKEN~RING/ETHERNET
~~,,,~_R_BB20_cc_DHCPBOOT~~
     where BB2ccDHC.CNF is a dummy file and cc is the two-character country code.
```

You do not have to add additional server record entries for DHCP boot. This one server record is sufficient for all types of adaptors.

In the workstation section of the file, there is a record for each configured client. The workstation record has the following format:

```
0080000123456 BPCLIENT1 ˜ FITS\BPCLIENT1 RIPLSRV Z ˜ ˜ ˜ ,,, ˜ R_BB20_cc_DHCPBOOT
     where cc is the two-character country code.
```

Understanding OS Server Record Identifier

The server record identifier is used to point to the server record that defines the network protocol stack a remote IPL client can use when connecting to the remote IPL server. The server record identifier must match field 12 of one of the server records in the RPL.MAP control file. In addition, the syntax convention for naming server record identifiers provides the following information:

```
                   - Enabled/Disabled state of the client
                   - The OS version that the client is to remote IPL
                   - The network adapter type and protocol stack that the
                     remote IPL client is to use
```

The server record identifier syntax for WorkSpace On-Demand is as follows:

```
s_BBvv_nn_aaappppp...   (maximum length is 48 characters)

            s  defines the state of the remote IPL client:

               R - indicates the client is enabled
               D - indicates the client is disabled

WorkSpace On-Demand clients can be created in the enabled or disabled state.

           vv  defines the major version ID of WorkSpace On-Demand:

               10 - indicates WorkSpace 1.0
               20 - indicates WorkSpace 2.0

           nn  defines the language ID version of
               WorkSpace On-Demand, for example:

               US - United States
               FR - France

          aaa  defines the network adapter type:

               OTK - indicates Token-ring
               OET - indicates Ethernet

       ppppp...defines a unique string that identifies
               the network adapter or protocol stack
               the remote IPL client is to use. This
               string must match field 4 of the adapter
               definition record in the NDISDD.PRO file.
```

The server record identifier syntax for other versions of OS/2 is as follows:

```
s_2vv_aaappppp...(maximum length is 48 characters)

              s  defines the state of the remote IPL client:

                 R - indicates the client is enabled
                 D - indicates the client is disabled

OS/2 clients are always created in enabled state.

             vv  defines the major version ID of OS/2:

                 0 - indicates OS/2 2.0
                 1 - indicates OS/2 2.1
                 30 - indicates OS/2 3.x
                 40 - indicates OS/2 4.0
             aaa  defines the network adapter type:

                  OTK - indicates Token-Ring
                  OET - indicates Ethernet
                  3CE - This is an old naming convention
                        originally used for 3COM ethernet
                        adapters. OET is the recommended prefix
                        for ethernet.

         ppppp... defines a unique string that identifies
                  the network adapter or protocol stack that the
                  remote IPL client is to use. The only
                  requirement for this string is that it
                  results in a unique server record identifier.
```

File Index Table (FIT)

A file index table (FIT) maps OS/2 and WorkSpace On-Demand workstation file names to server file names. A FIT can be thought of as a *mapping file*. A default FIT file and the FIT files for each machine are located on the server in the \IBMLAN\RPL\FITS\ directory. A FIT file is built for each client machine when you create it. Each client FIT file is defined in the workstation section of the RPL.MAP file. For 802.2 RIPL, the FIT file is sent to the requester as part of the boot block record during remote IPL. For DHCP PXE RIPL, the FIT file is downloaded as part of the first phase boot files during DHCP boot.

A FIT file consists of a header record specifying the name of the default network share where files can be found, followed by file name mapping records. The mapping records consist of two fields on the same line. The first field represents a file name, and the second represents the actual location of the file on the server.

These records consist of a prototype file name or prefix, followed by a space and an actual file name or prefix relative to the network share. If the prototype matches a proper prefix (part of the path name, ending in \) of the name to be matched, the matched portion is replaced by the actual prefix. If there is an exact match, it is used for substitution. If several prototypes match, the longest match is selected for substitution.

Network netnames can also be included as part of the substitution text. When this occurs, the netname on the first line is ignored. Specifying the network netname also provides the capability to use files and applications located on a server other than the default server.

A semicolon character (;) is used anywhere on a line of the FIT to begin a comment. Blank lines are ignored.

Using Wildcard Characters in the FIT File

The wildcard characters (?) and (*) are supported and are subject to the following rules:

- Wildcard characters can be placed only in the prototype file name field. They cannot appear in the target server name field.
- Wildcard references can be redirected only to the directory level. For example, the following field is valid:

  ```
  Z:\OS2\*.INI    \\ANYSRV01\WRKFILES\DEFAULT\OS2
  ```

  The following field is not valid:

```
Z:\OS2\*.INI    \\ANYSRV01\WRKFILES\DEFAULT\OS2\ANY.INI
```

- The ? and * cannot both be present in the same prototype file name field. For example, the following field is not valid:

```
Z:\OS2\ANY???.*  \\ANYSRV01\WRKFILES\DEFAULT\OS2
```

A brief example of a client FIT file follows. The lines are numbered here for reference; the line numbers are not displayed in the actual FIT file. In this example, ANYSRV01 is the remote IPL server name, and DEFAULT is the workstation name.

```
1) \\ANYSRV01\RPLFILES
2)
3) Z:\CONFIG.SYS            MACHINES\DEFAULT\CONFIG.SYS
4) Z:\OS2                   BB20.US\OS2
5) ; go to a different share
6) Z:\OS2\SYSTEM\SWAPPER.DAT \\ANYSRV01\WKRFILES\DEFAULT\OS2\SYSTEM\SWAPPER.DAT
7) Z:\                      \\ANYSRV01\WRKFILES\DEFAULT
```

Line **Description**

1 Defines the default remote IPL server and network share name.

2 Empty line.

3 Translates all references to Z:\CONFIG.SYS to:

```
\\ANYSRV01\RPLFILES\MACHINES\DEFAULT\CONFIG.SYS
```

Note that the default netname is automatically prefixed to the translated name.

4 Translates all references from Z:\OS2 to:

```
\\ANYSRV01\RPLFILES\BB20.US\OS2
```

Except for explicitly mapped file names, this record results in all Z:\OS2\*.* references being translated to:

```
\\ANYSRV01\RPLFILES\BB20.US\OS2\*.*
```

Subdirectory references are also mapped by this statement. For example, Z:\OS2\DLL\ANYFILE.DLL is translated to:

```
\\ANYSRV01\RPLFILES\BB20.US\OS2\DLL\ANYFILE.DLL
```

5 Comment

6 Translates all references from Z:\OS2\SYSTEM\SWAPPER.DAT to:

```
\\ANYSRV01\WKRFILES\DEFAULT\OS2\SYSTEM\SWAPPER.DAT
```

Note: In this example, the default netname is overridden by specifying the explicit UNC name. The translated file name is to the requester-unique file structure where the requester has read, write, create, delete, and execute access. Swapping here is defined on the remote server in comparison to local swapping.

7 Translates all other references to be relative to:

```
\\ANYSRV01\WRKFILES\DEFAULT
```

Note that the translated path is to the requester-unique file structure on the server that the requester has read, write, create, delete, and execute authority.

To add support for TCPBEUI protocol to 802.2 RIPL clients, the FIT file is extended with additional statements ending with @. Below is an example of a FIT file extension to support TCPBEUI.

```
; READONLY FILES

Z:\OS2\MDOS\VDMA.SYS   BB20.US\OS2\MDOS\VDMAAT.SYS

Z:\OS2\DLL\BVHVGA.DLL    BB20.US\OS2\DLL\BVHVGA.DLL @
Z:\OS2\DLL\DOSCALL1.DLL    BB20.US\OS2\DLL\DOSCALL1.DLL @
Z:\OS2\DLL\OS2CHAR.DLL   BB20.US\OS2\DLL\OS2CHAR.DLL @
Z:\OS2\DLL\QUECALLS.DLL  BB20.US\OS2\DLL\QUECALLS.DLL @
Z:\OS2\DLL\BVSCALLS.DLL  BB20.US\OS2\DLL\BVSCALLS.DLL @
Z:\OS2\DLL\BKSCALLS.DLL  BB20.US\OS2\DLL\BKSCALLS.DLL @
Z:\OS2\DLL\BMSCALLS.DLL  BB20.US\OS2\DLL\BMSCALLS.DLL @
Z:\OS2\DLL\SESMGR.DLL    BB20.US\OS2\DLL\SESMGR.DLL   @
Z:\IBMLAN\NETPROG\DHCPWAIT.EXE BB20.US\IBMLAN\NETPROG\DHCPWAIT.EXE @
Z:\IBMLAN\NETPROG\DHCPWAIT.SYM BB20.US\IBMLAN\NETPROG\DHCPWAIT.SYM @
Z:\IBMCOM\RFCADDR.EXE    BB20.US\IBMCOM\RFCADDR.EXE @
Z:\IBMCOM\PROTOCOL\TCPBEUI.SYM  BB20.US\IBMCOM\PROTOCOL\TCPBEUI.SYM @
Z:\IBMCOM\PROTOCOL\NBTCP.EXE    BB20.US\IBMCOM\PROTOCOL\NBTCP.EXE @
Z:\IBMCOM\RFCNAMES.LST   MACHINES\BH100\IBMCOM\RFCNAMES.LST @
Z:\MPTN\BIN\SETUP.CMD    MACHINES\BH100\MPTN\BIN\SETUP.CMD @
Z:\MPTN\ETC\DHCPCD.CFG   MACHINES\BH100\MPTN\ETC\DHCPCD.CFG @
Z:\MPTN\BIN\ROUTE.EXE    BB20.US\MPTN\BIN\ROUTE.EXE @
Z:\MPTN\BIN\ARP.EXE      BB20.US\MPTN\BIN\ARP.EXE @
Z:\MPTN\BIN\IFCONFIG.EXE BB20.US\MPTN\BIN\IFCONFIG.EXE @
Z:\MPTN\BIN\CNTRL.EXE    BB20.US\MPTN\BIN\CNTRL.EXE @
Z:\MPTN\BIN\IPGATE.EXE   BB20.US\MPTN\BIN\IPGATE.EXE @
Z:\MPTN\BIN\DHCPSTRT.EXE BB20.US\MPTN\BIN\DHCPSTRT.EXE @
Z:\MPTN\BIN\DHCPCD.EXE   BB20.US\MPTN\BIN\DHCPCD.EXE @
Z:\MPTN\BIN\SO32DLL.DLL  BB20.US\MPTN\DLL\SO32DLL.DLL @
Z:\MPTN\BIN\TCP32DLL.DLL BB20.US\MPTN\DLL\TCP32DLL.DLL @
Z:\MPTN\BIN\TCPIPDLL.DLL BB20.US\MPTN\DLL\TCPIPDLL.DLL @
Z:\MPTN\BIN\TCPMRI.DLL   BB20.US\MPTN\DLL\TCPMRI.DLL @
Z:\MPTN\BIN\TCPIP32.DLL  BB20.US\MPTN\DLL\TCPIP32.DLL @
Z:\MPTN\BIN\TCPTIME.DLL  BB20.US\MPTN\DLL\TCPTIME.DLL @
Z:\MPTN\MSG\NLS\DHCPSTRT.CAT BB20.US\MPTN\MSG\NLS\DHCPSTRT.CAT @
Z:\MPTN\MSG\NLS\DHCPMRES.DLL BB20.US\MPTN\MSG\NLS\DHCPMRES.DLL @
Z:\IBMI18N\DLL\SETLOC1.DLL  BB20.US\IBMI18N\DLL\SETLOC1.DLL @
Z:\IBMI18N\LOCALE\ENUS437.DLL  BB20.US\IBMI18N\LOCALE\ENUS437.DLL @
Z:\IBMI18N\LOCALE\ALIASES  BB20.US\IBMI18N\LOCALE\ALIASES @
Z:\IBMLAN\NETPROG\NET.MSG BB20.US\IBMLAN\NETPROG\NET.MSG @
```

User File Index Table (FIT)

There are also FIT files for each user that provide the same mapping function as remote IPL machine FIT files. However, User FIT files are specific to an individual User ID and are active only while that user is logged onto the client. The user FIT allows the in-memory FIT to be updated with user-specific FIT information. This allows the in-memory FIT to be dynamically changed without rebooting the client machine.

User FIT files are located on the Domain Controller in the `\IBMLAN\DCDB\USERS\username\` directory. A default User FIT file is located in the `\IBMLAN\DCDB\` directory. When a user logs on to a client, the client searches for a user-specific FIT file. If one is found, the in-memory copy of the machine FIT file is updated to add the user-specific FIT file entries. If the user-specific FIT file is not found, the default user FIT file is used.

Note: The default User FIT file is not required.

You can add entries to the default User FIT file or create user-specific FIT files, or both. The format for the user-specific FIT is the same format as any other FIT file except there cannot be a UNC name as the first entry. In User FIT files, all entries are file-mapping entries, comments, or blank lines. The following is an example of a User FIT mapping entry:

```
?:\ABCAPP\ABCFILE.EXT \\IBMLAN$\DCDB\USERS\ABCAPP
     where ? is replaced by the system as the boot drive of the client machine.
```

Note: User FIT files are primarily used to map files to the user area of the Domain Controller database, although they can be used to map files to any share a user can access.

You can place a special statement in the User FIT file to tell the system to also use the default User FIT file. Otherwise, only the user-specific FIT file is used. If the following line appears in the user-specific User FIT file, then the global User FIT file is also used:

```
 #include BB20ccDU.FIT
```

where cc is the country code.

Notes:

1. Regardless of the location of this line, the default User FIT file is processed last, after all of the user-specific User FIT file entries.
2. Only one #include is allowed.
3. There can be only one space between the #include and the default User FIT filename.
4. WorkSpace On-Demand 2.0 configurations may have servers running with different country codes and different levels of WorkSpace On-Demand. The remote IPL client that processes the #include statement will substitute the correct version and country code when it recognizes a default User FIT filename following #include.

NDISDD.PRO Control File

The NDISDD.PRO control file defines the network adapters that are supported for 802.2 RIPL and DHCP PXE RIPL. This file is located in the \IBMLAN\RPL directory and contains a definition record for each adapter type.

When you create a requester using the LAN Server Administration GUI, you select network adapters from those that appear in the listbox. The adapters that appear in the list are defined in the NDISDD.PRO file. When you install a new adapter, you can edit this file to provide the information that will appear in the GUI.

The following is an example of an NDISDD.PRO file, including a description of the fields. Fields 3, 4 and 5 apply only to WorkSpace On-Demand. If you include field 3 you must also include fields 4 and 5.

```
;NDIS device driver profile records are composed of 5 fields.
;They are described below.
;Field 1  This field specifies the DOS NDIS device driver name.
;Field 2  This field specifies the subdirectory name that contains the configuration file(s)
;         needed to remote boot the RIPL client.
;         d:\IBMLAN\RPL\IBMCOM\xxx contains the configuration files needed to RIPL OS/2 clients.
;         d - the drive on which the RIPL component has been installed
;         xxx - the text located in the second field of a given line
;Field 3  NIF file name for OS/2 device driver
;Field 4  CNF file name id reference for server record id
;Field 5  This field specifies the remote IPL protocol(s) a card may support
;         The possible types are 802.2 and DHCP boot
IBMTOK.DOS    TOKENRING    IBMTOK.NIF    OTKNTR    802.2
MACETH.DOS    ETHERNET     MACETH.NIF    OET       802.2
ELNKMC.DOS    ELNKMC       ELNKMC.NIF    OET3EM    802.2
```

```
ELNKII.DOS    ELNKII       ELNKII.NIF    OET3EI    802.2
IBMENI.DOS    ETHILAEI     IBMENI.NIF    OETLAE    802.2
F1MAC.DOS     ETHIPS2I
ELNK16.DOS    ELNK16       ELNK16.NIF    OET316    802.2
ELNK3.DOS     ELNK3        EL3IBM02.NIF  OET3E3    802.2
.
.
.
IBMTRP.DOS    TOKENTRP     IBMTRPO2.NIF  OTKTRP    802.2,DHCP
IBMFE.DOS     ETHERJ10     IBMFEEO2.NIF  OETFE     802.2,DHCP
```

When you are creating a requester using the LAN Server Administration GUI, the information in the third field in the adapter record is used by the server to build the CONFIG.SYS, PROTOCOL.INI, and SETUP.CMD files for the requester. The information in the fourth field is used to correlate to a server record in RPL.MAP when creating the workstation record for the requester. . The information in the fifth field of the record determines the boot method that will be enabled in the GUI for your selection.

Installing Remote IPL Using the OS/2 RIPLINST Utility

The RIPLINST utility copies the OS/2 operating system into a subdirectory on the OS/2 Warp Server or LAN Server. This copy is the central copy of the operating system that the clients use. All files required for remote IPL are copied into this subdirectory, including OS/2 device drivers and display short routines.

Each version of OS/2 has a unique version of RIPLINST. Most versions of RIPLINST have a different default target installation directory. The various default target installation directories are:

OS/2 version	**Target directory**
OS/2 3.0	*d*:\IBMLAN\RPL\OS2.30
OS/2 4.0	*d*:\IBMLAN\RPL\OS2.40

where *d*: indicates the drive where IBMLAN\RPL is installed.

This prevents an existing ..\OS2.xx directory tree from being overwritten automatically. To upgrade an existing..\OS2.xx directory tree, the target installation directory must be updated before starting the installation process. The target directory must be on the same drive where OS/2 remote IPL support was installed (this can be different from where OS/2 Warp Server or LAN Server was installed). The only part of the directory path that should be updated is the drive ID. Do not change any of the remaining path information.

After using RIPLINST to install OS/2 for remote IPL, run the updated version of the GETRPL utility (for more information, see the *Command Reference*).

The RIPLINST utility used to install the OS/2 code for OS/2 Warp Server or LAN Server remote IPL is located (in packed format) on diskette 7 of the OS/2 Installation diskettes.

Note: Use the OS/2 Installation diskette for the version of OS/2 that you want to install.

Use one of the following procedures to install and run RIPLINST:

- If your **server** operating system is the same as the version of OS/2 being installed by RIPLINST, see “Steps to Install RIPLINST” on page 223.

- If your **server** operating system is NOT the same as the version of OS/2 being installed by RIPLINST, see “Steps to Install RIPLINST on Different Version Server” on page 224.

Note: The OS/2 code on the OS/2 Warp Server SMP and OS/2 Warp Server for e-business CD-ROMs is not supported for remote IPL and cannot be installed by the RIPLINST utility.

For more information, see the following topics:

- “Steps to Install RIPLINST”
- “Steps to Install RIPLINST on Different Version Server” on page 224

Steps to Install RIPLINST

To install RIPLINST:

1. Do one of the following:
   - Insert the OS/2 Install diskette 7 into drive A. Then install RIPLINST by typing:
     ```
     UNPACK A:\RIPLINST
     ```
   - Insert the OS/2 Install CD-ROM into your CD-ROM drive. Then install RIPLINST by typing:
     ```
     UNPACK d:\OS2IMAGE\DISK_7\RIPLINST
     ```
     where *d* is your CD-ROM drive.

   The RIPLINST files are unpacked to the \OS2\INSTALL directory.
2. To start the RIPLINST program, go to an OS/2 window or full-screen session and type:
   ```
   RIPLINST
   ```
3. Press Enter to remove the title window.
4. The Change Source/Target window is displayed. In this window, you are provided the option to change the values for the following fields:

Field	**Value**
Source Directory	A:\
OS/2 RIPL Directory	*d*:\IBMLAN\RPL\OS2.*xx*

   where *d* is the drive where OS/2 Warp Server or LAN Server is installed and *xx* is the version of OS/2 installed.

   It is not necessary to change either of these options. It is assumed you are installing from a diskette drive. Change the source directory accordingly.

   Attention: The OS/2 remote IPL directory must be specified for the same drive where the Remote IPL service is installed. In addition, the base path of \IBMLAN\RPL must always be specified.
5. Select **Install**.
6. Insert diskettes as prompted.

Steps to Install RIPLINST on Different Version Server

To install RIPLINST on a different version server:

1. Create a temporary subdirectory by typing:

   ```
   MD TEMPRIPL
   ```
2. Change to the temporary subdirectory by typing:

   ```
   CD TEMPRIPL
   ```
3. Insert OS/2 Install diskette 2 into drive A.
4. Copy UNPACK.EXE to the TEMPRIPL directory by typing:

   ```
   COPY A:UNPACK.EXE
   ```
5. Check OS/2 Install diskette 2 for the file UNPACK2.EXE. If it is present, copy UNPACK2.EXE to the TEMPRIPL directory by typing:

   ```
   COPY A:UNPACK2.EXE
   ```

   Note: UNPACK2.EXE might not be present. If it is not on diskette 2, you do not need it.
6. Insert OS/2 Install diskette 7 into drive A.
7. Install the RIPLINST files by typing:

   ```
   UNPACK A:\RIPLINST d:\TEMPRIPL
   ```

   where *d* is the drive ID where TEMPRIPL is located.
8. Start the RIPLINST program by typing:

   ```
   RIPLINST
   ```

   Note: Each version of RIPLINST must use the corresponding OS/2 version of UNPACK and UNPACK2 (if it exists). Failure to do so results in one of the following error conditions:

   - RIPLINST traps while copying the W0F0000.BIO file.
   - The system locks up after displaying the copy window. You must reboot if this occurs.
9. Press Enter to clear the title window.
10. The Change Source/Target window is displayed. In this window, you are provided the option to change the values for the following fields:

Field	**Value**
Source Directory	A:\
OS/2 RIPL Directory	*d*:\IBMLAN\RPL\OS2.*xx*

    where *d* is the drive where OS/2 Warp Server or LAN Server is installed and *xx* is the version of OS/2 installed.

    It is not necessary to change either of these options. It is assumed you are installing from a diskette drive. Change the source directory accordingly.
11. Select **Install**.
12. Insert diskettes as prompted.

Supporting Multiple Levels of the OS/2 Operating System

It is possible to install and support multiple levels of the OS/2 operating system on a remote IPL server. This section documents the correct procedure to use to support such an environment.

To support multiple levels of the OS/2 operating system:

1. Run the OS/2 utility RIPLINST to install the OS/2 code in the RIPL directory tree. You must be careful to use the version of RIPLINST that matches the level of code to be installed.
2. After running RIPLINST, run the GETRPL utility (provided with OS/2 Warp Server and LAN Server) GETRPL uses information stored in the OS2SYS.INI file by RIPLINST so it is very important that GETRPL be run before using RIPLINST to install another version of OS/2.
3. Repeat steps 1 and 2 for each version of OS/2 to be remotely IPLed.
4. Check the \IBMLAN\RPL\RPL.MAP file. Look for the OS/2 server records, they start with yyyyyyyyyyyy or ;yyyyyyyyyyyy and the second field contains a name like OS230*.CNF or OS240*.CNF. A semicolon (;) in column 1 indicates the record is disabled. GETRPL enables or disables the appropriate records based upon what OS/2 version you installed.

Machines with Updatable IML Records

DBCS Note: The following statement about the Models 8556 and 8557 does not apply to you.

When using the Remote IPL service on any machine that has updatable initial microcode load (IML) records, perform the following modification to the remote IPL server. (Machines with IML records include Models 8556 and 8557.)

To update machines with IML records:

1. Copy the $0000000.IML file from the *Reference Diskette* to the IBMLAN\DCDB\IMAGES subdirectory.
2. Create a remote IPL image of the *Reference Diskette*. See “Creating a DOS Image from Diskette” on page 233 for instructions.
3. Edit the \IBMLAN\RPL\*xxyyy*.CNF file, where *xx* is the version of OS/2 installed and *yyy* identifies a network adapter type.
   a. Insert the following new line immediately before the lines starting with DRV:
      ```
      EXE C:\IBMLAN\RPL\DOS\IMLUPDAT.COM
      ```
   b. Save the file.
4. Edit the \IBMLAN\RPL\RPL.MAP file.
   a. Locate the workstation record for the workstation that requires the update.
   b. Update field 14 to specify the name of the *Reference Diskette* image you created at the beginning of this procedure.
   c. Save the file.
5. Restart the remote IPL workstation.

Chapter 17. Managing Remote IPL

After installing Remote IPL, the network administrator can create, customize, and manage Remote IPL clients. This chapter details some of the considerations regarding how to create and customize clients, along with the procedures for adding support for OS/2 SVGA and using the Remote IPL REXX commands.

For more information, see the following topics:

- "Creating, Changing, or Deleting a Remote IPL Client"
- "Customizing DOS Remote IPL Workstations" on page 231
- "Customizing OS/2 Remote IPL Workstations" on page 240
- "OS/2 SVGA Support for Remote IPL Clients" on page 244
- "Remote IPL REXX Procedures" on page 247

Creating, Changing, or Deleting a Remote IPL Client

Clients for OS/2, DOS, and WorkSpace On-Demand 1.0 and 2.0 can be created and maintained from the administration server. What follows are the basics for managing clients. For specifics in regard to WorkSpace On-Demand (about machine classes, for example), please refer to the *WorkSpace On-Demand 2.0 Administrator's Guide*.

For more information, see the following topics:

- Creating or Changing a Remote IPL Client
- Deleting a Remote IPL Client

Creating or Changing a RIPL Client

To create or change a client:

1. Open the **Connections** object on the Desktop.
2. Open **Network**.
3. Open **LAN Server Administration**.
4. Open the domain where the new client is to be created or changed. The icon for the domain object is a castle.
5. Open **Defined Servers**.
6. Open the RIPL server object where the new client is to be defined or changed.
7. Open the **Remote IPL Requesters** object. This folder contains, a generic Remote IPL template, templates for WorkSpace 1.0 and WorkSpace 2.0 requesters, and one icon for each requester currently defined.

At this point, the procedures for creating the different types of Remote IPL clients differ. Use one of the following procedures depending on the type of client you need:

- WorkSpace On-Demand
- OS/2 or DOS

WorkSpace on—Demand 1.0 and 2.0

To create or change a requester:

- To create a requester, drag and drop the **WorkSpace 1.0 or 2.0 Template** object to another location in the Remote IPL Requester folder. This adds a requester object to the folder and displays the **Settings** notebook. To use another requester as a template, select the requester object and press the right mouse button to display the menu. Then select **Create Another**. The **Settings** notebook is displayed.
- To change the properties of an existing requester, select the requester object you want to change, and then press the right mouse button to display the menu. Select **Properties**. The **Settings** notebook is displayed.

Fill in the pages on the WorkSpace On-Demand Template - Settings notebook:

1. Select the **Identity** page.
   a. When you create a requester it is enabled for remote IPL. You can disable a requester without deleting it and then enable it at any time. Select or clear the **Disable requester** check box. If the requester is currently running, disabling it does not take effect until the next time the requester is started.
   b. Complete the **Machine ID** field. The machine ID is an alphanumeric string containing up to 15 characters that you use to identify the requester.
   c. Complete the **Description** field. The description is an alphanumeric string of up to 48 characters that you use to describe the requester.
2. Select the **System** page.
   a. Select the **Boot drive ID** from the list. The default is Z:
   b. Select the **Operating system** from the list.
   c. Choose the location for the swap file. If the requester has a hard disk you can select **Local**. Otherwise, you must select **Remote** and the swap file will be on the server.
3. Select the **Hardware** page.
   a. Complete the **Network adapter address** field. This field is a unique address of the network adapter card. You can get this by turning on the requester machine and obtaining the character string following the AA entry on the display.
   b. Select a **Machine class** from the list. If the list does not include a machine class to support your specific hardware configuration, see the *WorkSpace On-Demand 2.0 Administrator's Guide*.
   c. The fields in the **Hardware Information** box allow you to choose network adapters, remote boot methods, and video selections. If the device support you need is not in the list, see the *WorkSpace On-Demand 2.0 Administrator's Guide*.
      1) Select a **Network adapter** from the list. The network adapter type you select determines the remote boot methods that are enabled for selection. If the adapter card supports both 802.2 RIPL and DHCP boot, both methods are enabled for selection, and RIPL is the default.
      2) Select a **Remote boot method**. **802.2 RIPL** and **DHCP boot** are enabled for selection if the network card you selected supports these boot protocols.
      3) Select a **Video monitor** from the list if your machine class supports this selection.

4) Select a **Video resolution** from the list if your machine class supports this selection.

You can press the **Reset all defaults** button if you want to change all entries back to the defaulted values.

4. Select the **Printers** page. You can add, change, or remove network or local printers.
   - To remove a network or local printer, select the desired printer from the list and select **Remove**.
   - To add a network or local printer, select **Add**, and then follow the steps below. You can configure up to four printers for any one client.
   - To change a network or local printer, select the desired printer from the list and select **Change**, and then follow the steps below.

   a. Complete the **Printer name** field. The printer name can be up to 25 characters.

   b. Select the desired **Port** from the list.

   c. Choose a **Resource** by selecting the desired **Attach using alias name** or **Attach using share name** button.

   d. If **Attach using alias name** is chosen, select the printer **Alias name** from the list.

   If **Attach using share name** is chosen, select the **Server name** and **Share name** from the lists.

   e. Select **OK**.
5. Select the **Protocols** page.

   a. Select a Network and Additional protocol.
   - Select **NetBEUI** or **TCPBEUI** as a network protocol to connect to the WorkSpace On-Demand server.
   - You can optionally select an additional protocol. These options are enabled according to the boot protocol selected.

   b. If you selected TCPBEUI as the network or additional protocol, you need to configure the TCPBEUI parameters:

   1) Select a **Node type** from the list. Broadcast node is the default.

   2) If you did not select broadcast node, you must fill in the remaining parameter fields:

   a) Enter **NETBIOS scope**. This can contain 128 characters in the format city.company.com.localscope.

   b) Enter the address of the **NETBIOS name server**. The address can contain up to 12 numeric characters in four groups of up to three characters each (for example, 123.123.123.123).

   c) Enter the address of the **Datagram distributor** server. The address can contain up to 12 numeric characters in four groups of up to three characters each (for example, 123.123.123.123).

   c. If you selected NetBEUI as the network protocol and the selected network adapter supports locally administered addressee, the Locally Administered Address will be enabled. This is a 13–character field that contains a locally administered network adapter address. The first character must be either an I for IEEE standard notation Ethernet address format, or T for IBM Token Ring Network format. The remaining 12 characters must be hexidecimal.
6. Select the **IP Address** page.

a. You must select **Configure TCP/IP** if you want to perform TCP/IP configuration. All other entries are disabled until you select this check box.

b. In the **Client address** box, select **Manual** for manual addressing, or select **Automatic using DHCP** for automatic addressing using dynamic host configuration protocol.

- If you select **Manual**, all entry fields are enabled. **Host name** is optional; all other fields are required.
- If you select **Automatic, using DHCP**:

  Optionally select **Also using DDNS**, dynamic domain name service, if you want DDNS in addition to DHCP.

  When **Automatic using DHCP** is selected, and **Also using DDNS** is checked, **Host Name** and **Domain name** are required; all other fields are disabled. If **Automatic using DHCP** is selected, but **Also using DDNS** is unchecked, then all the fields are disabled.

c. Complete the **Host name** field. The host name can contain up to 32 alphanumeric characters.

d. Complete the **Domain name** field. The domain name can contain up to 40 alphanumeric characters.

e. Complete the **IP address** field by entering the client's IP address. The IP address can contain up to 12 numeric characters in four groups containing up to three characters each (for example, 123.123.123.123).

f. Complete the **Router** field by entering the IP address of the router.

g. Complete the **Name server** field by entering the IP address of the Name server.

h. Complete the **Subnet mask** field.

Select **Set** to save the changes and close the notebook.

OS/2 or DOS Client

To create or change an OS/2 or DOS client:

1. Drag a copy of the Remote IPL Requesters template to an open area in the folder.

   The Remote IPL Requester notebook is displayed.
2. On the Identity page, select either **Enable DOS client** or **Enable OS/2 client**.

   Note: You must enable one of these clients before you can define or update any of the fields.

   You can disable a client without deleting it and then enable it at any time. Select or clear the **Disable requester** check box. If the client is currently running, disabling does not take effect until the next time the requester is started.
3. Complete the fields on the Identity page. For the network adapter address, refer to the documentation that came with the adapter to determine the adapter number.

   Note: You must specify a universally administered address in this field. Do not specify a locally administered address.
4. Select the **Parameters** tab.

   The Parameters page is displayed.
5. Select a server record identifier.

6. For a DOS remote IPL client definition, select an image ID from the drop-down list. If no IDs are listed, cancel the notebook and create an image. Several sample image definition files are shipped with the server. You can use one of these as a template for creating your image file. See “Understanding Image Definition Files” on page 232 for more information on this.

   Note: The diskette size and density information is not relevant in this situation. For example, STD3HHMA can be used in a client definition to remote IPL a client with the DOS 6 operating system, even if the client does not have a 3.5-inch high-density drive.

7. For an OS/2 remote IPL client definition, select a remote IPL startup drive.

   The remote IPL startup drive ID must be a letter from C through Z. If drive C is selected, and the remote IPL client has a local C drive, the local drive is automatically reassigned to the D drive. However, the startup drive ID should not duplicate any other drive letter installed on the remote IPL client local hard-disk drive.
8. Select **Create**.
9. After waiting several minutes to allow the NetLogon service to update the access control profiles on any additional servers, restart the Remote IPL service on each additional server. To restart the service, type the following command at an OS/2 command prompt on each additional server:

   ```
   NET START REMOTEBOOT
   ```

Deleting a RIPL Client

To delete a client in WorkSpace On-Demand, OS/2, or DOS:

1. Select the requester object you want to delete
2. Press the right mouse button to display the menu, and select **Delete** from the menu.

   A confirmation window is displayed
3. Select **Delete** or **Cancel**

Customizing DOS Remote IPL Workstations

The following information describes how to customize DOS remote IPL workstation features required by a more advanced user of remote IPL for DOS clients.

For more information, see the following topics:

- “Understanding Image Definition Files” on page 232
- “Creating a DOS Image from Diskette” on page 233
- “Creating a DOS Image from a Definition File” on page 233
- “Making a DOS Image on a Diskette” on page 234
- “Default Image Definition Files” on page 234
- “Sample DOS Remote IPL Data Files” on page 235
- “Updating Image Definition File Entries” on page 236
- “Upgrading DOS LAN Services IPL Images” on page 237
- “Using Custom Startup .BAT Files” on page 237
- “Using Custom NETWORK.INI Files” on page 239

- “Receiving Messages at a DOS Remote IPL Workstation” on page 239

Understanding Image Definition Files

You can update image definition files using either the Manage Images window in the LAN Server Administration or the MAKEIMG command. See *Command Reference* for more information.

Several sample image definition files are shipped with OS/2 Warp Server. You can use these files to build images for IBM DOS. For special situations and for some vendor versions of DOS, use these sample image definition files as templates to create and customize your own image definition files.

The following information explains how to create customized image definition files.

Image definition files have the same names as the images, plus a .DEF extension. They are stored in directory \IBMLAN\DCDB\IMAGES on the remote IPL server.

The following example shows the contents of sample image definition file STD3HFUL.DEF. The LAN Server Administration extracts the first line of the definition file as the description.

```
;      Standard IBM DOS LAN Services Program RIPL image
;      definition for a PC with 3.5" 1.4M A: diskette
;      with the full redirector
3.5/1.4M
?:\IBMLAN\DOSLAN\NET\STD_CFG.SYS CONFIG.SYS
?:\IBMLAN\DOSLAN\NET\STD_AUT.BAT AUTOEXEC.BAT
?:\IBMLAN\DOSLAN\NET\FULL_NET.INI NETWORK.INI
?:\IBMLAN\DOSLAN\NET\NET.EXE
?:\IBMLAN\DOSLAN\NET\NET.MSG
?:\IBMLAN\DOSLAN\NET\DLSHELP.SYS
?:\IBMLAN\DOSLAN\NET\CONNECT.EXE
```

A definition file contains the following types of information:

Comments Comments must start with a semicolon (;).

Blank lines Blank lines are ignored.

Diskette type A definition file can define a diskette image that emulates the diskette types that DOS LAN Services supports. This file must be specified in the first noncomment line of the definition file.

DBCS Note: In the following list, the only valid option for you is 3.5/1.44M.

Valid options are:

- 3.5/720K
- 3.5/1.44M
- 5.25/1.2M

File entries The remaining entries define file locations. These entries are explained in “Updating Image Definition File Entries” on page 236.

Note: If you are using UNC names in the image definition file shown previously, replace `?:` with `\\`*servername* (where *servername* is the server name) and replace `IBMLAN` with `IBMLAN$`.

Creating a DOS Image from Diskette

Use the following steps to create a DOS image from diskette.

To create a DOS image from diskette:

1. Insert the diskette in the local diskette drive.
2. On a DOS remote IPL server, open **LAN Server Administration**.
3. Open **Local Workstation**.
4. With mouse button 2, select **Diskette image source**.
5. From the pop-up menu, select **Make image**.

   The Make Image from Diskette window is displayed.
6. Type the image name.
7. Select the target server, which is the server where you want the image created.
8. Select the source drive, which is the local diskette drive.
9. Select **OK**.

   OS/2 Warp Server or LAN Server copies the image to the target server.

Note: You can also perform this task from the command line using the MAKEIMG utility.

Creating a DOS Image from a Definition File

If DOS Remote IPL Support is installed, you can also create images from image definition files. (Install DOS Remote IPL Support using the OS/2 Warp Server or LAN Server installation/configuration program. Refer to *Quick Beginnings* for more information.)

After DOS Remote IPL Support has been installed, you can create an image from a definition file.

To create an image from a definition file:

1. Open **LAN Server Administration**.
2. Open the appropriate domain object.
3. Open **Defined Servers**.
4. Open the appropriate remote IPL server object.
5. Open **DOS Image Definitions**.

   The DOS Image Definitions folder is displayed. It contains one object for each image definition that exists on the server.
6. With mouse button 2, select the definition object from which you want to make a DOS image.

   Note: The standard image definition files specify the diskette size and density information. For example, STD3HHMA can create a DOS image only on a workstation with a 3.5-inch high-density drive. However, an image created from the STD3HHMA image definition file can be used to remote IPL a client even if it does not have a 3.5-inch high-density drive.
7. From the pop-up menu, select the arrow to the right of **Make image→To server**.
8. Select the name of the target server, which is the server where you want the image created.
9. Select **OK**.

The image is created and saved in the\IBMLAN\DCDB\IMAGES directory on the target server.

Note: The target server you specify creates the image. Therefore, the required IPL Image Support must be installed at the destination server.

Making a DOS Image on a Diskette

If you are logged on to a server, you can use a default .DEF file to make a DOS image on a diskette. However, if you are logged on to a client, you must first replace the `?` in the default .DEF file with `\\` *`servername`*. The *servername* is the name of a remote IPL server in your domain.

To make an image on a diskette:

DBCS Note: In the following step, use the DOS 6.3/V system to prepare a system diskette.

1. Use the DOS 6.1 or higher operating system to prepare a system diskette. (Use the DOS FORMAT command with the /S option.) You must use a version of the DOS operating system that is the same as the version of DOS installed for DOS remote IPL on the selected program server where the image was created.
2. Open **LAN Server Administration**.
3. Open the appropriate domain object.
4. Open **Defined Servers**.
5. Open the appropriate remote IPL server object.
6. Open **DOS Image Definitions**.

   The DOS Image Definitions folder is displayed.
7. With mouse button 2, select the definition object that you want to make to diskette.
8. From the pop-up window, select the arrow to the right of **Make image→To diskette**.
9. Complete the fields on this window.
10. Ensure that the diskette you formatted in step 1 is inserted in the target drive.
11. Select **OK**.

    The DOS image is created on the diskette.

Default Image Definition Files

The following list names the standard definition files, with the diskette image for each. Each file creates a diskette image from files stored on the server's hard disk. This file produces an image including the minimum files required to connect a workstation to a program server.

STD3HBAS.DEF
3.5-inch 1.44MB image with basic redirector

STD3HFUL.DEF
3.5-inch 1.44MB image with full redirector

STD3LPRD.DEF
3.5-inch 1.44MB image with protect mode redirector

STD3HHMA.DEF
3.5-inch 1.44MB image with full redirector and high memory (HIMEM) support

STD3HUMB.DEF
3.5-inch 1.44MB image with full redirector and upper-memory block (UMB) support

STD3LBAS.DEF
3.5-inch 720KB image with basic redirector

STD3LFUL.DEF
3.5-inch 720KB image with full redirector

STD3HPRD.DEF
3.5-inch 720KB image with protect mode redirector

STD3LHMA.DEF
3.5-inch 720KB image with full redirector and high-memory support

STD3LUMB.DEF
3.5inch 720KB image with full redirector and upper-memory block support

STD5HBAS.DEF
5.25-inch 1.2MB image with basic redirector

STD5HFUL.DEF
5.25-inch 1.2MB image with full redirector

STD3HPRD.DEF
5.25-inch 1.2MB image with protect mode redirector

STD5HHMA.DEF
5.25-inch 1.2MB image with full redirector and high-memory support

STD5HUMB.DEF
5.25-inch 1.2MB image with full redirector and upper-memory block support

Sample DOS Remote IPL Data Files

The following list describes the files in the sample Image Definition File. If DOS remote IPL was selected during installation, these files exist only if DOS LAN Services is installed. These files are installed on each server configured to support the Remote IPL service and are used with the standard image definitions:

File **Description**

STD_AUT.BAT
This file includes commands in the AUTOEXEC.BAT file for a remote IPL workstation initializing DOS LAN Services. The file is renamed to AUTOEXEC.BAT when it is included in the diskette image. The file resides in the \IBMLAN\DOSLAN\NET directory.

STD_CFG.SYS
This file includes example configuration commands for the DOS 3.3 environment of the remote IPL workstation. This file is renamed to CONFIG.SYS when included in the diskette image. This file resides in the \IBMLAN\DOSLAN\NET directory.

To use the IBM LAN Support Program on the remote IPL workstation, do not specify the device driver entries in the

CONFIG.SYS file. The Remote IPL service sends device drivers to the workstation before running the CONFIG.SYS file.

DBCS Note: The following example is based on a U.S. English system.

The following example shows the contents of the STD_CFG.SYS file.

```
COM /E:2000 /PLASTDRIVE=˜˜˜˜˜˜B
FILES=30
BUFFERS=10
FCBS=16,8
DEVICE=A:\VDISK.SYS 10 128 16˜˜˜˜˜˜3
```

Note: LASTDRIVE indicates drives reserved for DOS LAN Services use. The LASTDRIVE value must always be at least F in order to start DOS LAN Services and should be greater than the last disk partition or virtual drive created. Increase the drive letter by one increment for hard-disk-based DOS clients and two increments for remote IPL or diskette-based clients. The default LASTDRIVE value is Z.

Updating Image Definition File Entries

Each line entry in the image definition file defines the actual location, on the remote IPL server, of a file or directory that is to be accessed by way of the DOS client. You might need to update an image definition file to load new device drivers added to the CONFIG.SYS or AUTOEXEC.BAT files. A definition entry has the following format:

```
<path><source_name.ext1><destination_name.ext2>
```

The following example shows an entry from the STD3HFUL.DEF file:

```
?:\IBMLAN\DOSLAN\NET\STD_CFG.SYS   CONFIG.SYS
```

In a line entry, <*path*> is the DOS path. For example, in the previous example, <*path*> equals the following:

```
?:\IBMLAN\DOSLAN\NET
```

Because this path can be interpreted from the machine you are using when you make an image, you normally do not need to specify a drive. Two facilities allow you to specify the directory containing files to include:

- A drive specified as `?:` (as in the example) means the drive where OS/2 Warp Server is installed on the remote IPL server where the image is built. All files specified in the standard definitions on your domain controller are installed on each remote IPL server.
- You can specify a path using a UNC name:

  ```
  <\\servername\netname\path>\<filename>
  ```

  For example:

  ```
  \\IPLSRVER\IBMLAN$\DOSLAN\NET
  ```

  This specification allows you to build an image on one server if the source files reside on another server. In this example, the directory is a UNC name for the source files, where IBMLAN$ is a netname on the source server IPLSRVER.

To use this facility, source files must be present on the source server before building an image through Manage Images or MAKEIMG.

The remaining two components of the entry format are defined as follows:

```
path><source_name.ext1><destination_name.ext2>
<; comment if required>
```

- < *source_name.ext1*> is the file name in the directory. An example is STD_CFG.SYS. If this field is not specified, files in the subdirectory are copied into the diskette image with their names unchanged.
- < *destination_name.ext2*> is the file name as it is stored in the diskette image. An example is CONFIG.SYS. If this field is not specified, the file is included in the diskette image with its name unchanged. A path cannot be specified for the source or destination file because a diskette image built from a definition file cannot include subdirectories.

The definition file can also include comments wherever needed, as long as every comment entry is on a line by itself and has a semicolon character (;) at the beginning of the line.

The following DOS system files do not need to be included in the definition file lines because they are included automatically from the server where the image is built:

- IBMBIO.COM
- IBMDOS.COM
- COMMAND.COM

The following IBM LAN Support Program device driver files are loaded in the boot block and do not need to be listed in the image file:

- DXMA0MOD.SYS
- DXMC *x*MOD.SYS
- DXMT0MOD.SYS
- DXMG *x*MOD.SYS
- DXME0MOD.SYS
- DXMJ0MOD.SYS

Upgrading DOS LAN Services IPL Images

Existing remote IPL or DOS LAN Services image diskettes must be rebuilt whenever a new version of the DOS operating system or DOS LAN Services is installed on the remote IPL server.

When you upgrade the version of DOS being remote IPLed, you cannot upgrade the current DOS files or images using a DOS upgrade version. You can use only the full release versions of DOS to make remote IPL images.

Using Custom Startup .BAT Files

Each remote IPL workstation can have a different startup sequence by using different .BAT files. You can provide custom startup .BAT files by using any of the following methods:

- Including different .BAT files in the individual diskette images accessed by different remote IPL workstations
- Using the parameter substitution mechanism in a diskette image accessed by different remote IPL workstations

- Using the parameter substitution mechanism to run different .BAT files (external to the diskette image) from the AUTOEXEC.BAT file. In this way, different .BAT files can be run from a single diskette image.

The remote IPL feature has a parameter substitution mechanism. This mechanism allows parameter values specified in the client definition section of the RPL.MAP file to be included in commands as part of any file in a diskette image (for example, CONFIG.SYS or AUTOEXEC.BAT).

The following sample AUTOEXEC.BAT file illustrates remote IPL parameter substitution:

DBCS Note: The following example is based on a U.S. English system.

```
NET START RDR˜˜˜˜˜˜˜2˜˜˜˜˜˜˜6 /RPL
NET LOGON * */DOM:˜˜˜˜˜˜˜6
NET USE D:\\˜˜˜˜˜˜˜5\IBMLAN$:

SET CURIMAGE = ˜˜˜˜˜˜˜4
```

Variables consisting of tilde characters (˜) with a hexadecimal digit specify which parameter values come from the remote IPL workstation's entry in the RPL.MAP file. The variables must include at least 5 tilde characters to trigger the substitution mechanism. The number of tilde characters plus the digit must be greater than or equal to the total number of characters in the substituted parameter.

The hexadecimal digit following the tilde string denotes the field number from which the parameter value comes.

The /RPL parameter specifies that this client is a remote IPL client rather than a client started from its hard disk.

For example, the first command in the previous AUTOEXEC.BAT file example (NET START RDR) has the following meaning:

> Start the DOS LAN Services redirector function using the remote IPL workstation's network name as specified in field 2 of the RPL.MAP entry for that remote IPL workstation. (The maximum expected size of the redirector name is 15 characters.)

This command becomes:

```
NET START
```

if REQ001 is the name specified in field 2 and DOMAIN1 is the name specified in field 6 of the RPL.MAP entry for the remote IPL workstation.

The second command in AUTOEXEC.BAT becomes:

```
NET LOGON * * /DOM:DOMAIN1
```

if DOMAIN1 is the name specified in field 6 of the RPL.MAP entry for the remote IPL workstation. This command provides an opportunity to logon to domain DOMAIN1 by prompting the user for a user ID and password.

Similarly, the third command in AUTOEXEC.BAT becomes:

```
NET USE D: \\SRV0\IBMLAN$
```

if SRV0 is the name specified in field 5 of the RPL.MAP entry for the remote IPL workstation.

Notes:

1. All copies of .BAT files used from remote clients must have their read-only attribute set or must reside in a directory with access control profile permissions of RX (read, execute) defined for it.

   Similarly, all programs run from such .BAT files must also be read-only or must reside in a directory with access control profile permissions of RX (read, execute) defined for it. Failure to meet either of these two criteria causes the DOS operating system to signal a sharing violation if more than one remote IPL workstation tries accessing the same file concurrently.
2. Each remote IPL workstation entry in the RPL.MAP file can include up to 15 fields. Fields E and F are not used by the default remote IPL configuration. They can be used for parameter substitution by specifying the correct hexadecimal digit in the substitution variable.

Using Custom NETWORK.INI Files

You can create customized NETWORK.INI configuration files for your DOS Remote IPL clients. Unlike other files, you cannot specify a customized NETWORK.INI file to use during startup in an image definition file. This is because the Remote IPL service installs a default NETWORK.INI file for clients upon initial startup. Additional steps to replace the default NETWORK.INI file with the custom NETWORK.INI file are required after rebooting the workstation.

The following steps allow DOS Remote IPL client workstations to access a customized NETWORK.INI file.

To create access to customized NETWORK.INI files:

1. Copy the customized NETWORK.INI file onto the\IBMLAN\DOSLAN\NET subdirectory of the Remote IPL server.
2. Remote IPL to start the client workstation. This creates a connection to the server subdirectory\IBMLAN\DOSLAN\NET using the Z: drive.
3. Copy the custom NETWORK.INI file from the server onto the client’s Y: drive by using the COPY command. The following example assumes the client machine name is SIMPSON. The commands are issued at the client workstation:
   a. Type `Y:` and press Enter.
   b. Type `CD SIMPSON` to change to the directory for SIMPSON located on the server and press Enter.
   c. Type the following command to copy the custom NETWORK.INI file into the SIMPSON directory:

      ```
      COPY Z:\IBMLAN\DOSLAN\NET\custom.ini NETWORK.INI
      ```

      where *custom.ini* is the name of the customized NETWORK.INI file.

After the file is copied to the DOS client, the customized NETWORK.INI file is used to start the workstation instead of the default file.

Receiving Messages at a DOS Remote IPL Workstation

Use the following instructions to create an image that allows a remote IPL workstation to receive messages.

To create an image definition file for DOS remote IPL workstations receiving messages:

1. Create a new .DEF file by copying an existing file.
2. Modify the copy of the .DEF file as follows:
   a. The file will contain one of the following entries:
      - `?\IBMLAN\DOSLAN\NET\FULL_NET.INI`
      - `?\IBMLAN\DOSLAN\NET\BASICNET.INI`
      - `?\IBMLAN\DOSLAN\NET\PRDR_NET.INI`

      Change the entry in your file to:

      ```
      ?\IBMLAN\DOSLAN\NET\xxxxxNET.INI
      ```

      where *xxxxx* is the name of the new .INI file.

      Note: Remember the original file name (FULL_NET.INI, PRDR_NET.INI, or BASICNET.INI) because you use it later in this procedure.

   b. Add the following entry to the .DEF file:

      ```
      ?\IBMLAN\DOSLAN\NET\MESSENGR.EXE
      ```

      Note: To add the Message Pop-Up feature, add another entry:

      ```
      ?\IBMLAN\DOSLAN\NET\NETPOPUP.EXE
      ```
3. Copy the .INI file (either FULL_NET.INI, PRDR_NET.INI, or BASICNET.INI) that was listed in your original .DEF file to the *xxxxx*NET.INI file, where *xxxxx*NET.INI is the file name that you specified in the new .DEF file.
4. Add `messenger` to the **autostart** parameter in the *xxxxx*NET.INI file.

   Note: To start the Message Pop-Up feature, add `netpopup` to the **autostart** parameter in the *xxxxx*NET.INI file. For example, type:

   ```
   autostart=full messenger netpopup
   ```
5. To create a message log file, add the following entry to the *xxxxx*NET.INI file:

   ```
   logfile=d:\filename
   ```

   where *d* is a local (nonredirected) drive to the *xxxxx*NET.INI file and *filename* is the file name and extension for the message log file. You cannot log messages to a remote drive.

Customizing OS/2 Remote IPL Workstations

Each OS/2 remote IPL workstation has its own CONFIG.SYS, PROTOCOL.INI, and IBMLAN.INI files, but it uses a central copy of the OS/2 operating system and OS/2 LAN Requester software. (DOS remote IPL workstations use a central copy of the DOS operating system and DOS LAN Services initialization files.)

The following information describes other modifications you need to make to the CONFIG.SYS and *machineid*.FIT files.

If you want these changes to apply to all the remote IPL clients, make the changes to the default files before you create the remote IPL clients. The default files are:

```
\IBMLAN\RPL\FITS\DEFALT20.FIT
\IBMLAN\RPL\MACHINES\DEFALT30\CONFIG.DEF
\IBMLAN\RPL\MACHINES\DEFALT40\CONFIG.DEF
\IBMLAN\RPL\IBMCOM\adaptertype\OS2\PROTOCOL.INI
```

The *adaptertype* parameter is based on the type of network as follows:

DBCS Note: PCNET and PCNETA in the following list do not apply to DBCS systems.

Value	Network
3C0XPCI	3Com Fast EtherLink/EtherLink XL Family OS/2
ELNK16	3Com EtherLink 16 (3c507) Family — OS/2
ELNK3	3Com EtherLink III (3c509) Family — OS/2
ELNK II	3Com EtherLink II (3c503) Family — OS/2
ELNKMC	3Com EtherLink/MC (3c523) Family — OS/2
ETHERJ10	IBM 100/10 EtherJet PCI Adapter (OS/2)
ETHERJET	IBM EtherJet ISA Ethernet Adapter (IBMEINDI.OS2)
ETHERNET	IBM PS/2 Adapter for Ethernet Networks
ETHILAE	IBM LAN Adapter/A for Ethernet (IBMENII.OS2)
ETHILAEI	IBM LAN Adapter/A for Ethernet (IBMENI.OS2)
ETHIPS2I	IBM PS/2 Adapter for BNC/UTP Ethernet Networks
IBM_CLA	Crystal LAN CS8900/CS8920 Ethernet Adapter
IBM_E100	Intel 10/100 Ethernet
MADGE	Madge FastMac OS/2 NDIS driver for Smart 16/4 Ringnodes
SMCTOK	SMC TokenCard elite for OS/2 (SMC 8115)
TOKENRING	IBM T-R Shared RAM Family (UP/SMP, IBMTOK.OS2)
TOKENTRP	IBM PCI Token-Ring Adapter (IBMTRP.OS2)
TOKN1641	IBM Token Ring Network 16/4 Adapter II (IBM16TR.OS2)
TOKNLS32	IBM LANStreamer 16/32 MCA Adapter (IBMMPC.OS2)
WDPLUS	SMC Ethernet ISA Adapter Family (SMC8000.OS2)

Note: Before modifying the default files, create a backup copy.

For more information, see the following topics:

- “Using a Model to Create Remote IPL Workstations”
- “Specifying Mouse Types” on page 243
- “Installing Printer Drivers” on page 243
- “Updating Master OS/2 OS2.INI Files” on page 244
- “Other CONFIG.SYS Options” on page 244

Using a Model to Create Remote IPL Workstations

When creating OS/2 remote IPL client definitions, you can create a typical definition that can be used as a model when defining other workstations. Modeling allows you to customize OS/2 remote IPL client definitions for a specific group of similar workstations. The necessary changes are made only once to the model definition. After the changes to the model files are complete, you can create new remote IPL client definitions that contain these changes. Modeling can also be used to customize the CONFIG.SYS file, the PROTOCOL.INI file, *machineid*.FIT file, the OS2.INI file, and other files for remote IPL workstations.

To illustrate how modeling works, assume that you have a group of remote IPL workstations with XGA displays. Because the IBM-supplied default definition assumes a VGA display, you can create a model definition for an XGA client and then use it to create remote IPL definitions for other workstations with XGA displays. The following example illustrates the modeling procedure.

To create a model remote IPL client definition:

1. Create an OS/2 remote IPL client definition, for example, XGAMODEL, using the procedures in “Creating, Changing, or Deleting a Remote IPL Client” on page 227.
2. Use the RPLSETD utility to configure the XGAMODEL workstation for XGA support.

   ```
   RPLSETD /C:XGAMODEL /D:IBMXGA32
   ```

   See “RPLSETD.CMD REXX Procedure” on page 247 for more information.
3. Start the remote IPL model client.
4. Customize the desktop.
5. Shut down the remote IPL model client to set the new configuration.

To create a remote IPL client definition using the model definition for an XGA display:

1. Open **LAN Server Administration**.
2. Open the appropriate domain object.
3. Open **Defined Servers**.
4. Open the appropriate server object.
5. Open **Remote IPL Clients**.
6. Select the **XGAMODEL** object.
7. Press mouse button 2, and select **Create another**.

   The Remote IPL Client notebook is displayed.
8. Modify the fields on the Identity page as necessary:
   a. In the **Machine ID** field, type the name of the remote IPL client. Replace the model name with the workstation name.
   b. For the network adapter address, use the value you got in step 1 or refer to the documentation that came with the adapter to determine the adapter number. The 12-digit hexadecimal address is displayed when the client is turned on. This address is preceded by *AA* on the display.

      Note: You must specify a universally administered address in this field. Do not specify a locally administered address.
9. Select **Create**.

   The new OS/2 remote IPL workstation is created using the same CONFIG.SYS and FIT files that were customized for the model XGAMODEL client definition.
10. After waiting several minutes to allow the NetLogon service time to update the access control profiles on any additional servers, restart the Remote IPL service on each additional server. To restart the service, type the following command at an OS/2 command prompt on each additional server:

    ```
    NET START REMOTEBOOT
    ```

Notes:

1. Because some files are locked by the OS/2 program when the system is running, the client being used as a model must not be active.
2. Systems with remote IPL client definitions based on the same model must have the same type of network adapter.

Specifying Mouse Types

By default, remote IPL workstations assume that a PS/2 mouse is connected to the pointing device port. If a client is using a different mouse, modify \IBMLAN\RPL\MACHINES\ *clientname*\CONFIG.SYS and make the following updates.

To specify a different mouse type:

1. Add the appropriate device-dependent driver statement before the DEVICE=Z:\OS2\MOUSE.SYS statement. For example:

   ```
   DEVICE=Z:\OS2\PCLOGIC$ SERIAL=COM1
   ```

2. Update the DEVICE=Z:\OS2\MOUSE.SYS statement and add the TYPE parameter. For example:

   ```
   DEVICE=Z:\OS2\MOUSE.SYS TYPE=PCLOGIC$
   ```

Installing Printer Drivers

Use the next procedure to install a printer driver.

To install a new printer driver on an OS/2 remote IPL workstation:

Replace the default path in the Install New Printer Driver window from A:\ to C:\OS2\DLL\ *xxxx*, where *xxxx* is one of the following directories:

DBCS Note: The following example is based on a U.S. English system.

Directory Name	**Printer Device Drivers**
EPSON	Epson, Panasonic, and Hewlett Packard drivers
HP\PCL\LASERJET	Laserjet drivers for Epson, Hewlett Packard, IBM, Kyocera, and Panasonic
IBM4019	IBM 4019 drivers
IBM42XX	IBM 2380, 2381, 2390, 2391, 4201, 4202, 4207, 4208, 4224, and 4226 drivers
IBM52012	IBM 52012 driver
IBM52XX	IBM 3816, 5202, and 5204 drivers
IBMNULL	IBM Null driver
PLOTTERS	IBM and Hewlett Packard plotter drivers
PMPLOTPD	PMPLOTQPR driver
PSCRIPT	IBM, Apple, and Hewlett Packard drivers
SMGXPJET	Paintjet* drivers

See the *OS/2 Desktop Guide* for more information on installing a new printer driver.

Updating Master OS/2 OS2.INI Files

Some users have a customized master OS2.INI file that is copied to the client directory each time the client is started with remote IPL. This master file must also be updated to identify the type of display driver that the client workstation is using. Clients with different display types (such as VGA, XGA, 8514) MUST use different master OS2.INI files.

To update a master OS2.INI file, enter the following command:

```
RPLRXUTL  /D:DISPLAY_DRIVER /C:INI_FILENAME
```

where:

D:DISPLAY_DRIVER
The same as for the RPLSETD command.

C:INI_FILENAME
The drive, path, and filename of the master OS2.INI file to be updated.

For example:

```
RPLRXUTL /D:IBMVGA32 /C:E:\IBMLAN\RPL\MASTER\VGAOS2.INI
```

The RPLRXUTL utility does not display error information, but does display a non-zero return code if an error occurs. If you need to verify error information, start RPLRXUTL from a CMD procedure (batch file or REXX) so that the return code can be tested.

Other CONFIG.SYS Options

To improve system performance, reorder the LIBPATH statement, the DPATH statement, and the PATH statement in the CONFIG.SYS file to list the directories from most frequently used to least frequently used. If the client has a hard disk, delete REM from the beginning of the DISKCACHE statement in the CONFIG.SYS file.

OS/2 SVGA Support for Remote IPL Clients

Limited SVGA support is provided for OS/2 Warp 3.0 and 4.0 remote IPL clients.

The SVGA support has the following prerequisites:

- OS/2 REXX support.
- IBM PS/ValuePoint machines used as remote IPL clients must be at BIOS level L6ET53A or later.

Note: Only SVGA video drivers provided with the base operating system are supported in the remote IPL environment. Other SVGA video drivers, for example, drivers found on an electronic bulletin board service (BBS), are not supported for remote IPL.

For more information, see the following topics:

- “Installing OS/2 SVGA Support on the Remote IPL Server” on page 245

- “Configuring a Remote IPL Server/Client for OS/2 SVGA Video Support”

Installing OS/2 SVGA Support on the Remote IPL Server

To install OS/2 SVGA support on the remote IPL server:

1. Run the “RPLSVGAI.CMD REXX Procedure” on page 248 for each OS/2 version that is installed in the remote IPL directory tree. RPLSVGAI can determine from Display Driver diskette 1 which OS/2 version is being updated.

   If diskettes are used as the source, RPLSVGAI prompts you for the appropriate OS/2 Display Driver diskettes. The OS/2 Warp Display Driver diskettes are in XDF diskette format. The remote IPL server must support the XDF format before RPLSVGAI can be used to install the OS/2 Warp SVGA support files.
2. Start the server and log on as an administrator.
3. Run GETRPL.

   GETRPL creates the access control profiles for these directories. If you are running 386 HPFS, you do not need to do this step.

Configuring a Remote IPL Server/Client for OS/2 SVGA Video Support

Configuring a remote IPL client for SVGA video support is a two step process. First, the remote IPL client definition on the remote IPL server must be updated. Second, the remote IPL client must use the appropriate OS/2 install function to install the SVGA support. The following sections provide step by step instructions for these two functions.

For more information, see the following topics:

- “Creating a Remote IPL Client Definition for OS/2 SVGA Support”
- “Installing OS/2 SVGA Support on the Remote IPL Client” on page 246

Creating a Remote IPL Client Definition for OS/2 SVGA Support

Perform the following procedure at the remote IPL server.

To create a Remote IPL client definition for OS/2 SVGA support:

1. Create an OS/2 remote IPL client.
2. Use RPLSETD to reconfigure the client to allow SVGA support.

For example, to configure a ISA bus machine called MACH01, use the following command:

```
RPLSETD /C:MACH01  /D:SVGA  /B:ISA
```

For a description of the RPLSETD options, see “RPLSETD.CMD REXX Procedure” on page 247.

When the /D:SVGA or S3SVGA option is specified, the RPLSETD utility does not configure the client for SVGA. It modifies the client definition so that the remote IPL client can run the OS/2 Selective Install program.

Notes:

1. SVGA support requires that each remote IPL client have a unique copy of several display-related files. Ensure that there is enough free space on the hard

disk where \IBMLAN\RPLUSER is installed to allow each SVGA workstation to have a copies of the display files in addition to the normal hard disk requirements for a remote IPL client.

2. Configuring a workstation for SVGA moves the workstations CONFIG.SYS file from the \IBMLAN\RPL\MACHINES\client directory to the \IBMLAN\RPLUSER\client directory. The workstation has write access to this file and could potentially modify it in such a fashion that the workstation could no longer be IPLed remotely.

Installing OS/2 SVGA Support on the Remote IPL Client

Perform the following procedure on the remote IPL client.

To install OS/2 SVGA support on the remote IPL client:

1. Start the remote IPL client.
2. Open **System Setup**.
3. Select **Selective Install**.
4. Select **Primary Display**, and then select **OK**.

   The Primary Display Adapter Type window is displayed. The detected SVGA adapter is highlighted.
5. Select **OK**.

   The Monitor Configuration/Selection Utility window is displayed.
6. Select **Install Using Defaults for Monitor Type** and then select **OK**.

   The screen appears blank for a few seconds, and then either a Screen Resolution Selection window or the Source Directory window is displayed.
7. If the Screen Resolution Selection window is displayed, select the appropriate resolution.
8. The Source Directory window is displayed. Ensure that the default source (*d*:\OS2\DISP where *d*: is the boot drive) is highlighted.

   Select **Install**.

   The selected video support is installed. Depending on the video adapter, you might be prompted for additional information such as the desired display resolution.

   For OS/2 Warp, a window is displayed requesting the Microsoft Windows 3.1 diskettes. Change the **Source** field to be *d*:\OS2\DISP where *d*: is the boot drive (default is Z:). Use this same source path for any additional Windows diskettes requested.

   A Display Driver Install information window is displayed indicating that shutdown is required before the changes become effective.
9. If non-S3 SVGA support was installed, shut down the system and restart it. If you were not prompted to select a display resolution during the install (step 6), continue with the following steps after the system restarts.

   If S3 SVGA support was installed, continue with the following steps.
10. Open **System Setup**.
11. Open **System**.

    The System Properties notebook is displayed.
12. Select the desired display resolution.
13. Depending on the video adapter installed, the Screen page might have a Page 2 that allows you to configure a specific display for your workstation.
14. Shut down and restart the system to use the new display support.

Remote IPL REXX Procedures

The following sections provide information relating to changes in REXX procedures that are used by remote IPL. For more information about these and other utilities, see the *Command Reference*.

For more information, see the following topics:

- "RPLSETD.CMD REXX Procedure"
- "RPLSVGAI.CMD REXX Procedure" on page 248

RPLSETD.CMD REXX Procedure

The RPLSETD.CMD procedure provides the following functions:

- Upgrades existing remote IPL clients to use the appropriate video device driver. RPLSETD determines the version of the target OS/2 and automatically select the appropriate video device driver.
- Updates a remote IPL client to perform an IPL on a different version of OS/2. The OS/2 code must be installed in the remote IPL directory structure.
- Updates a remote IPL client to change the bus type, as in MCA or ISA/PCI/EISA.
- Updates a remote IPL client to specify whether the swap path and WIN-OS/2 paging file is on a local hard disk or on the remote IPL server.
- Updates an OS/2 Warp 4 remote IPL client to support TCP/IP.

Using a RPLSETD Response File

To use the response file option, do the following:

1. Create an ASCII file that contains the appropriate keyword values.

   The valid response file entries/keywords are:

```
; Comment line
[GROUP]  (this statement is optional for the first group
         and required for all subsequent groups)
DISPLAYDRIVER=
CLIENT=
CLIENTLIST=
CURRENTOS2DIR=
NEWOS2DIR=
BUSTYPE=
SWAPTARGET=
TCPIP
```

   A ; (semicolon) in column 1 indicates the line is a comment.

   Leading blanks are allowed on keyword statements.

   The keywords are defined in the *Command Reference* syntax description.

   [GROUP] designates the start of a remote IPL client or group of clients that share the same configuration characteristics. When the [GROUP] statement is encountered, the client machine(s) in the previous group are updated according to the specified keyword(s). Multiple [GROUP]s can appear in the response file. This allows a single response file to process a number of different configurations. The [GROUP] statement is optional for the first group in the response file but is required for all subsequent groups.

CLIENT and CLIENTLIST are equivalent and multiple entries can be specified on either. Multiple CLIENT and CLIENTLIST keywords can be specified per group. Only one of each of the other keywords is allowed per group.

2. Type the following command:

   ```
   RPLSETD /R:d:\path\response_filename
   ```

   where *d*:\ *path*\ *response_filename* is the fully qualified file name of the response file.

Example:

```
[GROUP]             (optional)
; Update existing clients to support the IBMXGA32 display
; driver, switch from OS2.20 to OS2.30, support the MCA bus,
; and put the swap path on a local hard disk.
CLIENT=DEFALT20
CLIENT=MACH001,MACH002
CLIENTLIST=MACH003,MACH004
DISPLAYDRIVER=IBMXGA32
CURRENTOS2DIR=OS2.20
NEWOS2DIR=OS2.30
BUSTYPE=MCA
SWAPTARGET=L

[GROUP]              (required)
; Update client for ISA bus and put the swap path on the remote IPL
; server (no local hard disk). Enable TCPIP support
CLIENT=MACH005
BUSTYPE=ISA
SWAPTARGET=S
TCPIP
```

RPLSVGAI.CMD REXX Procedure

Before a remote IPL client can be configured for SVGA support, additional OS/2 SVGA support files must be installed. A special utility, RPLSVGAI.CMD, is provided to install this support.

The syntax for RPLSVGAI.CMD is:

```
RPLSVGAI  [/S:sourcepath]  [/L:logfile]
```

- where *sourcepath* specifies where to look for the SVGA support files. The default is A:\. However, it can be any of the following:
  - A diskette drive, for example, A:\
  - The root directory of an OS/2 Warp diskette image tree created by the OS/2 SEIMAGE.EXE utility, for example, C:\CID\OS2WARP3 or C:\CID\OS2WARP4.
  - The root directory of an OS/2 Warp diskette image tree on the OS/2 Warp Server CD-ROM; for example, *d*:\OS2IMAGE.
- where *logfile* specifies a fully qualified file name to be used to log any error messages.

RPLSVGAI must be run for each OS/2 version (OS /2 Warp 3.0 or 4.0) that is installed in the remote IPL directory tree. RPLSVGAI can determine from Display Driver diskette 1 which OS/2 version is being updated.

If diskettes are used as the source, RPLSVGAI prompts you for the appropriate OS/2 Display Driver diskettes. The Warp Display Driver diskettes are in XDF diskette format. The remote IPL server must be updated to support the XDF format before RPLSVGAI can be used to install the OS/2 Warp SVGA support files.

Chapter 18. The Uninterruptible Power Supply Service

An uninterruptible power supply (UPS) is a battery connected to a server that keeps the server running during an electrical power failure. If power to the server is interrupted, this battery keeps the server running until either the UPS service can manage a safe shutdown or until an administrator stops the server.

The UPS battery must be connected to a serial port for the UPS service to provide automatic shutdown. See the battery manufacturer's instructions for information about how to install the UPS.

For more information, see the following topics:

- "Using the UPS Service"
- "Configuring the UPS Service" on page 252

Using the UPS Service

During a power failure, the UPS service immediately pauses the Server service to prevent any new connections. It then sends out an alert that a power failure has occurred. The UPS service waits an interval of time specified by the **messdelay** parameter in the UPS section of the IBMLAN.INI file. If power is restored during this interval, another alert is sent, informing the administrator that power has been restored.

Note: The Messenger service and Network Message utility must be running for UPS-based alerts to be displayed as soon as they are sent. If these services are not started, you are not alerted to power failures at the server.

If power is not restored during the interval specified by the **messdelay** parameter, the UPS service warns users who have sessions with the server to end their sessions and displays a message at the server advising that all sessions will be closed.

The UPS service notifies users and administrators that a shutdown is imminent. The service repeats this alert at intervals specified by the **messtime** parameter in the UPS section of the IBMLAN.INI file. These alerts continue until power is restored, the server receives a low-battery signal from the battery (which means the battery is about to run out of power), or until the battery timer expires.

If power is restored, all users are sent an alert that power is restored, and normal operations are resumed.

If the server receives a low-battery message while the power is satisfactory, the UPS service responds as specified by the **lowbattery** parameter. If the server receives a low-battery signal while the power is not available, or if the battery timer expires, the UPS service does the following (see Figure 22 on page 255):

1. Informs all users of the server of the impending server shutdown
2. Stops all OS/2 Warp Server or LAN Server network services
3. Closes the file system

Before the UPS service stops the server and client, OS/2 Warp Server or LAN Server uses the **cmdtimer** parameter to determine the time in which to run a .CMD batch program. For example, you can set up a .CMD batch program to close any open application files. The .CMD path and file are specified by the **cmdfile** parameter in the UPS section of IBMLAN.INI.

Configuring the UPS Service

If a server has a UPS battery installed, make the UPS service one of the services that starts automatically with the Server service. This way, the UPS service is running if there is a power failure at the server. For information about installing and configuring the UPS service, see the *Command Reference* .

All time intervals and options that the UPS service uses are configurable. These options are listed in the following table. See the *Command Reference* for information on how to start the UPS service from the OS/2 command line.

Note: The configuration options for the UPS service are contained in the UPS section of the IBMLAN.INI file.

Option **Description**

batterymsg Specifies the interval of time used to repeat alerts for a low battery condition. This parameter is valid only when the **lowbattery** parameter is set to either WARNING or SHUTDOWN and a low battery signal is received while the AC line current is still satisfactory. The range is from 30 seconds to 3600 seconds. The default is 600 seconds.

batterytime Specifies the number of seconds the server can run on a battery before the UPS service initiates shutdown. Use this optional entry only if no low-battery signal is available. The range is 0 to 28800. The default is 60 seconds.

cmdfile Specifies a .CMD batch program of commands to be run before the server shuts down. The path name can be either absolute or relative to the OS/2 Warp Server or LAN Server directory (IBMLAN).

cmdtimer Specifies the number of seconds the UPS service gives the .CMD file to complete processing. The range is 0 to 600 seconds. The default is 30 seconds. If the .CMD file does not finish execution within the specified number of seconds, an error is logged.

devicename Specifies the name of the device for the server to open. This entry must be set to UPS_DEV.

lowbattery Specifies the response by the UPS service if the UPS signals that its battery power is low but the AC line current is satisfactory. If this parameter is set to WARNING, the UPS service generates repeated warnings (using the time interval set by the **batterymsg** parameter) to alert recipients, identifying the affected server. If this parameter is set to SHUTDOWN, the UPS services shuts down the affected server after warning the server’s local users and alerting users who have active sessions with the server. For both WARNING and SHUTDOWN, the event is recorded in the error log. If the **lowbattery** parameter is set to DISABLE, the event is recorded in the error log and no alert is generated. The default is WARNING.

messdelay Specifies the number of seconds between initial power failure and the first message sent to users. No messages are sent if power is restored within this interval. The range is 0 to 120. The default is 5 seconds.

messtime
Specifies the number of seconds between messages sent to users notifying them of a power failure. The range is 30 to 300. The default is 120 seconds.

recharge
Specifies the number of minutes of recharge time required for each minute of battery run time. This optional entry is used only if no low-battery signal is available. The range is 5 to 250 minutes. The default is 100 minutes.

signals
Specifies the signals available from the battery. The value is a 3-digit binary number. For information about the signals the battery sends and receives, see the manual supplied with the battery.

- The first digit is either 1 if the battery can signal the UPS service upon power failure or 0 if it cannot. The default is 1.
- The second digit is either 1 if the battery can signal the UPS service of a low battery condition (usually 2 minutes of power remaining) or 0 if it cannot. The default is 0.
- The third digit is either 1 if the battery can accept a shutoff signal from the UPS service or 0 if it cannot. The default is 0. If the third digit is 1, the UPS service conducts an orderly shutdown of the OS/2 Warp Server or LAN Server software, and the battery stops providing backup power. When the battery detects power restoration, it restarts the workstation.

Note: If neither of the first two digits of **signals** is set to 1, the UPS service does not start.

voltlevels
Specifies the voltage levels for the signals listed in the **signals** option. The value is a 3-digit binary number. For information about signal voltage, see the manual supplied with the battery.

- The first digit is either 0 if the battery uses negative voltage or 1 if it uses positive voltage to signal the UPS service of a power failure. The default is 1.
- The second digit is either 0 if the battery uses negative voltage or 1 if it uses positive voltage to signal the UPS service that there is less than 2 minutes of power remaining. The default is 0.
- The third digit is either 0 if the battery recognizes negative voltage as the shutoff signal or 1 if it recognizes positive voltage as the shutoff signal. The default is 0.

Note: If the low battery voltage level is not set correctly, the UPS service does not start.

For more information, see the following topics:

- “Configuring the UPS Device Driver”
- “UPS Scenarios” on page 254

Configuring the UPS Device Driver

The UPS device driver communicates with the UPS through a serial port. The OS/2 Warp Server or LAN Server installation and configuration program sets the PORT parameter of the device driver to either COM1 or COM2. The device driver can be further configured if those ports are not available.

The CONFIG.SYS statement can be changed as follows:

```
device=path>\netprog\upsdrv.os2/IOADDR:xxxx /IRQ:x/PORT:COMx
```

where:

path Specifies the drive and path to the installed IBMLAN tree.

/IOADDR: *xxxx*
Specifies the port address of the serial device. This number can be 1 to 4 hexadecimal digits. For this value, refer to the documentation for the serial device.

/IRQ: *x* Specifies the interrupt level associated with the serial device. This number must be 1 hexadecimal digit. For this value, refer to the documentation for the serial device.

/PORT:COM *x* Specifies the number of the serial port. The value for *x* must be either 1 or 2.

Note: You must specify the IOADDR and IRQ parameters together. You cannot use this combination with the PORT parameters.

The following example installs the UPS device driver on a machine equipped with a dual-async adapter:

```
device=d:\ibmlan\netprog\upsdrv.os2 /IOADDR:3220 /IRQ:3
```

Hardware diagnostics indicates that the second port of the adapter uses interrupt level 3 and I/O address 3220. The UPS device is attached to the port, and OS/2 Warp Server or LAN Server is installed on drive D.

UPS Scenarios

Figures Figure 22 on page 255 and Figure 23 on page 256 show two possible scenarios for the UPS service.

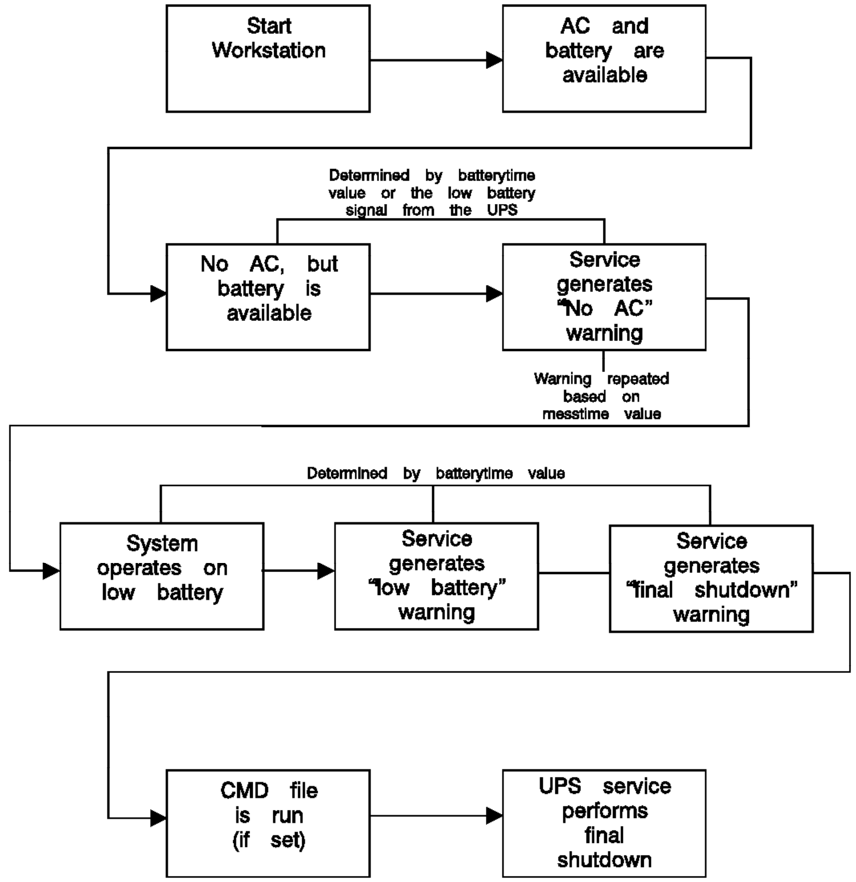

Start Workstation
AC and battery are available
Determined by batterytime value or the low battery signal from the UPS
No AC, but battery is available
Service generates "No AC" warning
Warning repeated based on messtime value
Determined by batterytime value
System operates on low battery
Service generates "low battery" warning
Service generates "final shutdown" warning
CMD file is run (if set)
UPS service performs final shutdown

Figure 22. Flowchart of UPS Running with No Electricity and a Good Battery

Note: Figure 23 on page 256 assumes that the **lowbattery** parameter is set to SHUTDOWN. If **lowbattery** is set to WARNING, then alerts are generated, but the UPS service does not shut down the server.

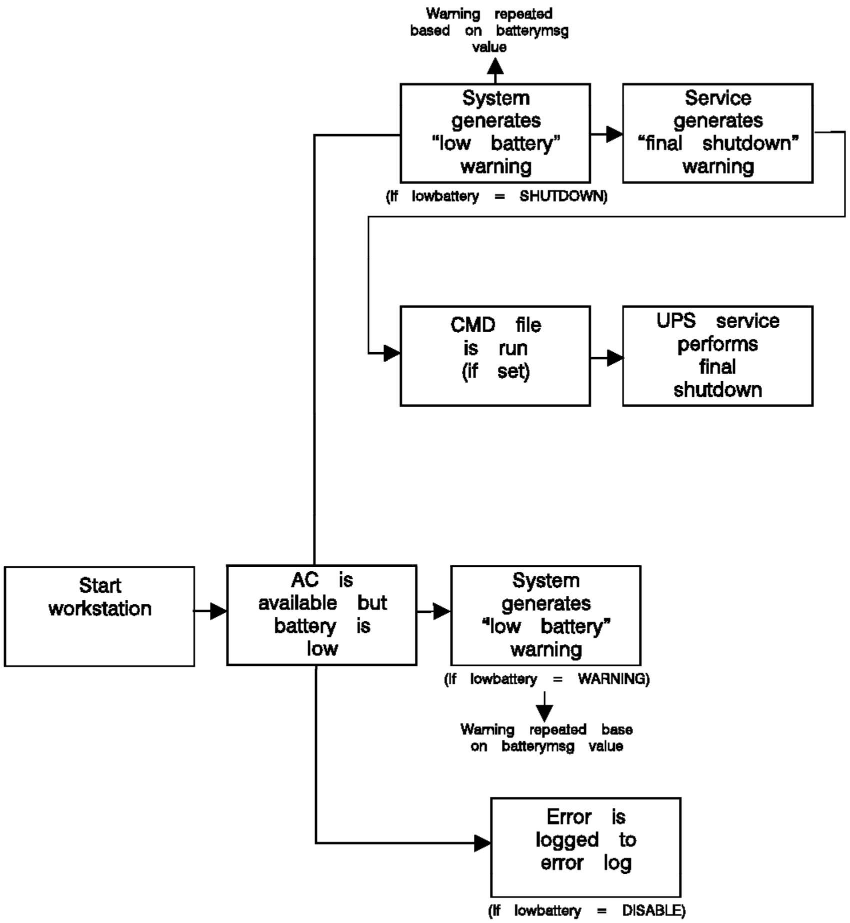

Warning repeated based on batterymsg value
System generates "low battery" warning
(If lowbattery = SHUTDOWN)
Service generates "final shutdown" warning
CMD file is run (if set)
UPS service performs final shutdown
Start workstation
AC is available but battery is low
System generates "low battery" warning
(If lowbattery = WARNING)
Warning repeated base on batterymsg value
Error is logged to error log
(If lowbattery = DISABLE)

Figure 23. Flowchart of UPS Running with Electricity but a Low Battery During Startup

Note:

1. If your UPS unit provides low-battery signaling, the **batterytime** parameter is not used. If your UPS unit does not provide low-battery signaling, ensure that digit 2 of the **signals** parameters is set to 0, which activates the **batterytime** parameter. The **signals** parameter is set to 100 by default.
2. To set the correct **recharge** parameter value for your particular UPS unit, refer to the manufacturer's documentation accompanying your UPS unit.
3. The UPS service works with contact closure-type UPS devices. However, voltage-sensing serial devices, such as the RS-232, must detect voltage transitions (from positive to negative and negative to positive) on the serial port pins to function correctly. Ensure that the UPS cable that you are using is capable of correctly signalling this type of port.

Appendix A. Directory Structure

This appendix lists the contents for the following directories:

- MUGLIB (for UPM)
- Requester IBMLAN
- Server IBMLAN
- Server IBMLAN with remote IPL
- Domain control database (\IBMLAN\DCDB)

Notes:

1. For information on the IBMCOM directory (for LAN Adapter and Protocol Support), see the *MPTS Configuration Guide*.
2. The IBM386FS directory is in the root directory of the boot drive. It contains the 386 HPFS files and the Fault Tolerance files.

For more information, see the following topics:

- “MUGLIB Directory Contents”
- “Requester IBMLAN Directory Contents”
- “Server IBMLAN Directory Contents” on page 258
- “Server IBMLAN Directory Contents for Remote IPL” on page 259
- “Domain Control Database Directory Contents” on page 260

MUGLIB Directory Contents

Below is a list of the subdirectories of a server’s MUGLIB directory. MUGLIB is also used for OS/2 Warp Server or LAN Server UPM support.

Subdirectory	**Contents**
\DLL	Network dynamic link libraries (all .DLL files)
\ACCOUNTS	UPM files

Note: If OS/2 Warp Server or LAN Server is not already installed on the server, the installation program copies the NET.ACC file from \MUGLIB\ACCOUNTS (if it exists) to \IBMLAN\ACCOUNTS. If the NET.ACC file does not exist, the default file on the OS/2 Warp Server or LAN Server installation diskette is copied to \IBMLAN\ACCOUNTS.

Requester IBMLAN Directory Contents

The following are the subdirectories of a requester’s IBMLAN directory.

Subdirectory	**Contents**
IBMLAN.INI	OS/2 configuration parameters for this requester
\BACKUP	Backup of existing configuration files
\INSTALL	Installation/configuration program
\BOOK	Online publications
\NETLIB	Network dynamic link libraries

\NETPROG	Network programs and user interface modules
\SERVICES	Network services available on the requester
\LOGS	Error log and message log
\ACCOUNTS	User Profile Management files
\NETSRC\H	API header files
\NETSRC\LIB	API libraries
\REPL	Empty at installation
\REPL\IMPORT	Default import path for the Replicator service (empty at installation)

Note: Deleting the MESSAGES.LOG file in the \LOGS subdirectory without first stopping the Messenger service causes the message log file to stop accepting new entries. To avoid this loss of entries,first stop the Messenger service temporarily with the command`NET LOG /OFF` . After deleting the message log file, resume the service by typing`NET LOG /ON` .

Server IBMLAN Directory Contents

Below is a list of the subdirectories of a server’s IBMLAN directory.

DBCS Note: In the following list, the contents of the\DOSLAN\DOS subdirectory is the code for versions 5.0, 5.0\V, and 6.*x* \V of the DOS operating system (optional).

Subdirectory	**Contents**
IBMLAN.INI	Configuration parameters for this server
\INSTALL	Installation/configuration program
\BOOK	Online publications
\NETLIB	Network dynamic link libraries
\NETPROG	Network programs and user interface modules
\SERVICES	Network services on the server
\LOGS	Error logs, message log, audit trail log, and FTADMIN log
\ACCOUNTS	User Profile Management files
\ACCOUNTS\USERDIRS	Logon information (empty at installation)
\ACCOUNTS \USERDIRS\SCRIPTS	Logon information (empty at installation)
\NETSRC\H	API header files
\NETSRC\LIB	API libraries
\USERS	Users’ home directories. These subdirectories are not automatically deleted when the associated user ID is deleted.
\REPL	Empty at installation
\REPL\EXPORT	Default export path for the Replicator service (empty at installation)

\REPL\IMPORT	Default import path for the Replicator service (empty at installation)
\REPL\IMPORT \SCRIPTS	Default directory used by NetLogon services
\DOSLAN	DOS LAN Services code (optional)
\DOSLAN\DOS	DOS versions 3.3, 5.0, 6.x code (optional)
\DOSLAN\NET	DOS LAN Services programs (optional)
\DOSLAN\LSP	LAN Support Program files (optional)
\XPG4	Translation utility for OS/2 Warp Server or LAN Server
\XPG4\LOCALE	Translation support for OS/2 Warp Server or LAN Server

Server IBMLAN Directory Contents for Remote IPL

Below is a list of the subdirectories that are added to the server's IBMLAN directory if remote IPL is installed.

Subdirectory	Contents
\RPL	Main remote IPL directory
\RPL\FITS	File index tables (FIT) for OS/2, DOS, and WorkSpace On-Demand remote IPL workstations. Default FIT files are located here.
\RPL\DOS	DOS remote IPL programs and loader
\DCDB\IMAGES	DOS image files for DOS remote IPL workstations, image DEF files of domain controller
\RPL\IBMCOM	Subset of IBMCOM directory that OS/2 remote IPL workstations use, which contains CONFIG.SYS and PROTOCOL.INI files
\RPL\IBMLAN	Subset of IBMLAN directory that OS/2 remote IPL workstations use
\PROFILES	SRVAUTO.PRO, which defines the shares used by OS/2 and DOS Remote IPL
\RPL\OS2.30	OS/2 3.0 installed code for remote IPL workstations
\RPL\OS/2.40	OS/2 4.0 installed code for remote IPL workstations
\RPL\BB10.[COUNTRY]	Installed code for WorkSpace On-Demand 1.0
\RPL\BB20.[COUNTRY]	Installed code for WorkSpace On-Demand 2.0
\RPL\MACHINES	Workstation directories containing workstation-specific files, including configuration files (read-only files)
\RPL \MACHINES\DEFALT20	IBMLAN.INI and other files for default users for OS/2; 2.0

\RPL \MACHINES\DEFALT21
IBMLAN.INI and other files for default users for OS/2; 2.1

\RPL\MUGLIB User Profile Management (UPM) programs for all remote IPL workstations

\RPLUSER User-specific remote IPL directory for all remote IPL workstations

\RPLUSER\DEFALT *xx*
User-specific writable OS/2 Warp Server, LAN Server, LAN Adapter and Protocol Support, and OS/2 files for the default user

Domain Control Database Directory Contents

The domain control database exists in directory IBMLAN\DCDB on the domain controller. Below are the subdirectories of IBMLAN\DCDB.

Subdirectory **Contents**

\DATA DCDB and access control profiles

\FILES .CMD or .BAT files for external files resources

\DEVICES .CMD or .BAT files for external serial device resources

\PRINTERS .CMD or .BAT files for external printer resources

\APPS .CMD or .BAT files to start applications

\IMAGES .IMG (image) and .DEF (image definition) files

\LISTS DOS LAN Services list files

\USERS *userid*
User profiles (for example, `\USER1`, `\USER2` `\USERn`). Each user profile contains the following:

For a user at an OS/2 requester:

- USER.A — Lists the user’s private applications
- USER.S — Lists what is displayed on the user’s Public and Private Applications objects
- USER.L — Lists the user’s logon assignments
- PROFILE.CMD — Contains commands that run automatically when the user logs on. You create this optional file.

For a user at a DOS requester:

- LIST.A — Lists the user’s private applications
- LIST.S — Lists what is displayed on the user’sLAN server application
- LIST.U — Lists the user’s logon assignments
- PROFILE.BAT — Contains commands that run automatically when the user logs on. You create this optional file.

Appendix B. User Profile Management

This appendix discusses how you can manage users and groups throughUser Profile Management as in previous versions of OS/2 Warp Server and LAN Server. In OS/2 Warp Server, you can also use LAN Server Administration as described in "Chapter 5. Managing Users and Groups" on page 43.

You can perform more user and group management functions from the OS/2 Warp Server Administration than you can from theUser Profile Management interface. Some of the functions available only from LAN Server Administration are:

- The capability to define up to 16,000 users per domain
- User and group ID cloning

  Cloning saves time by allowing you to use your mouse to take existing user and group objects and make clones (copies) that can be renamed and changed as required.
- Drag and drop enablement for logon assignments and for user and group definitions

  You can drag and drop aliases into user and group objects to automatically create logon assignments. In addition, you can drag and drop user accounts into groups or groups into user accounts to automatically update a user or group definition.
- Ability to define home directories for users

  You can specify home directories on the server for a user's personal use.
- Ability to enforce directory limits on users

  You can set size limits on home directories and enforce them so users cannot exceed them. Alerts are sent to the users when the space used is nearing the limit.

After you install OS/2 Warp Server, you must define new users to the network so they can log on and access network resources. Groups are defined for access and messaging purposes. This appendix describes how to define and manage users and groups and how to create guest accounts.

The following tasks for managing users are discussed:

- Adding users
- Granting and revoking operator privileges
- Updating user information
- Deleting a user
- Creating a Logon profile
- Updating Logon assignments
- Updating public applications on users' program starters
- Assigning a home directory
- Setting a user password expiration period for the domain

The following tasks for managing groups are discussed:

- Adding a group
- Viewing a group
- Updating a group
- Deleting a group

For more information, see the following topics:

- “Domain User and Group Definitions”
- “What is User Profile Management?”
- “Managing Users” on page 264
- “Managing Groups” on page 271

Domain User and Group Definitions

OS/2 Warp Server allows the user and group definitions file, created and updated through User Profile Management, to be centralized. This file is named NET.ACC and is maintained on the domain controller. Whenever a change is made to the user and group definitions, the NET.ACC file is sent from the domain controller to all servers that are running the NetLogon service in the domain. The NetLogon service allows a server to receive a copy of the user and group definitions file (NET.ACC).

LAN Requesters do not get copies of the NET.ACC file changes. Therefore, if user and group definitions are needed locally for an application (such as database manager), users must also be defined on the LAN Requester workstation through User Profile Management for the database manager requirements.

When the user and group definitions file is updated, the NET.ACC file is not immediately replicated to the additional servers on the domain. The time it takes to update depends on when the update is made in relation to the value specified with the **pulse** parameter in the NetLogon section of the IBMLAN.INI file. This value indicates how often (in seconds) the NET.ACC file is replicated to the additional servers.

You can log on to a domain and make changes to user and group definitions from any workstation on the network. The changes are made to the master copy at the domain controller and then sent to all servers that are running the NetLogon service.

With OS/2 Warp Server, the user and group definitions file is maintained centrally at thedomain controller. These definitions are used at each workstation in the domain running OS/2 Warp Server.

OS/2 Warp Server also allows users with Accounts operator privilege to manage users. *Accounts operators* can create new users, modify user accounts, and manage group definitions. However, they cannot create or manage administrators or other operators. See “Granting and Revoking Operator Privileges” on page 266 for more information.

What is User Profile Management?

User Profile Management (UPM) is the OS/2 Warp Server or LAN Server component that provides the means of managing users and groups:

- User ID validation. Each installation of User Profile Management is local to the particular workstation where it is installed and validates users who access controlled data or use programs that reside on that particular workstation.

- The mechanism for users to log on to the system and log off from the system and to identify and authenticate system users.

For more information, see the following topics:
- “User Profile Management Character Sets”
- “National Language Support Restrictions” on page 264

User Profile Management Character Sets

OS/2 Warp Server identifiers defined in User Profile Management are *user IDs*, *group IDs*, and *passwords*. The maximum length of each identifier is:

user IDs	20
group IDs	20
password	14
domain name	15
machine ID	15

Note: The following characters are not allowed in these fields through the UPMACCTS interface:

```
" / \ : [ ] | < > + = ; , * ?
```

OS/2 Warp Server uses an *expanded character set*, which consists of printable characters. (National Language Support users should see “National Language Support Restrictions” on page 264.)

The following rules apply to the use of the character set:

- The minimum number of characters (bytes) for the password depends on the **minpwlen** parameter on the NET ACCOUNTS command. However, in OS/2 Warp Server and IBM Extended Services database manager, all identifiers are restricted to 8 characters (bytes).
- User IDs and group IDs cannot have the following values:
  - USERS
  - LOCAL
  - GUESTS
  - ADMINS
  - PUBLIC
  - RPLGROUP

Notes:

1. IBM Extended Services Communications Manager and database manager identifiers are restricted to the minimal character set. Communications Manager identifiers, however, can be from 1 through 10 bytes if the UPMCSET command is run with the \E parameter.
2. The logon process may be unable to log on or access resources if the code page or country code of the system differs from those specified when the identifier was created. It is the user’s responsibility to make sure the expanded character set is used only when the code page and country code of the system are not changed.

National Language Support Restrictions

National Language Support (NLS) users at DOS LAN Services may not be able to use all characters included in the User Profile Management expanded character set. Follow the DOS guidelines for acceptable accented characters except for the following:

COUNTRY or LANGUAGE	PERMITTED CHARACTERS
France (FR)	A — Z, 1 — 9, and nonalphabetics
Canadian French (CF)	A — Z, 1 — 9, and nonalphabetics
Portugal (PO)	A — Z, 1 — 9, Ñ, and nonalphabetics
Spain (SP)	A — Z, 1 — 9, Ñ, Ç, and nonalphabetics
Latin America (LA)	A — Z, 1 — 9, Ñ, and nonalphabetics
Japan	A — Z, 1 — 9, nonalphabetics, Kanji, Hiragana, and Katakana
Korea	A — Z, 1 — 9, nonalphabetics, Hanja, and Hangeul
Taiwan	A — Z, 1 — 9, nonalphabetics, and Hanzi

Managing Users

For these procedures, you are making changes to the user and group definitions file for the *current domain*. You can only complete OS/2 Warp Server user and group tasks that require the User Profile Management, such as giving users logon assignments, in the current domain. To make changes to another domain's user and group definitions file without logging on to that domain, select **Use domain** from the User Profile Management Actions pull-down menu and then select the domain to administer. Your user ID and password must be the same on any domain you select to administer through the **Use domain** function.

For more information, see the following topic:

- "Adding a User"
- "Granting and Revoking Operator Privileges" on page 266
- "Updating User Information" on page 267
- "Deleting a User" on page 269
- "Creating a Logon Profile" on page 269
- "Updating Logon and Desktop Application Assignments" on page 270

Adding a User

You must add a user to the domain before that user can access the network. You can add approximately 1260 users for each domain. The actual maximum is determined by the length of the user IDs and comments in the file. If your user IDs are brief and your user comments fields unused, you may be able to add as many as 1800 users to the domain. If you exceed the limit, UPM Services does not display the additional users. You can use the NET USER command to define more than 1800 users on a domain; however, you may not be able to view all of the user definitions through User Profile Management.

To add a user:

1. On the desktop, select **User Profile Management Services**.
2. Select **User Profile Management** from the UPM Services folder.
3. In the User Profile Management–User Profile window, select **Manage** from the menu bar.
4. Select **Manage Users** from the Manage pull-down menu.
5. The User Profile Management–User Management window lists all users defined to the current domain. Select **New** from this list.
6. Select **Add a new user ID** from the Actions pull-down menu.
7. Complete the Add a New User window with the information describing the new user. The user ID should not be the same as the machine ID.
   - Select **User** or **Administrator** (a LAN network administrator) to specify the user type. If you select **User**, you can also specify whether the user should have accounts operator privilege.

     Of the user types definable through User Profile Management, only the user and administrator types are significant to OS/2 Warp Server. A third User Profile Management user type is *local administrator*. A local administrator has database manager authority (SYSADM) for local databases (residing on that user's machine) but has only user privileges on the OS/2 LAN. In contrast, a network administrator has network administrator authority and database manager SYSADM authority for all databases on the LAN. For further information on the local administrator user type, see "Database Manager Considerations when Adding Users".
   - In the **Password** box, specify whether a password is required. The password can be from 4 through 14 characters (bytes) long. If you select **Password Required**, you can also select **Expire Password** if you want to force the user to change the password at the first logon.

     Because the password is not displayed when you type it, you are prompted to type the password a second time to confirm it.

     If you select **Password Optional**, the user can later choose to add a password without intervention by the administrator.
   - The **Logon** box lets you allow or deny logon to individual users on the domain. If you select **Denied**, you can give the user access authority later by changing this field to **Allowed**.

For more information, see the following topic:

- "Database Manager Considerations when Adding Users"

Database Manager Considerations when Adding Users

To access databases on a remote Database Manager server, you must have an administrator or local administrator ID defined at the database client so that you can update the directories. You can use the default administrator ID supplied at installation or one you created.

However, if you are installing OS/2 Warp Server on the same workstation with the database client, then you must have an administrator ID defined on the network or a local administrator ID defined at the database client. The local administrator ID should be the same as your domain user ID.

The local administrator user type must be defined at the local workstation on which the user is a local administrator. To access databases on a remote Database Manager server, there must be one (and only one) local administrator user type defined at each Database Manager client. This definition differs from the LAN user types user and administrator, which can be defined remotely. Because the local administrator user type is tied to the machine ID, it cannot be defined remotely.

To create a local administrator user ID at a workstation:

1. If you are logged on to the domain, first log off, either by selecting **Logoff** from UPM Services or by typing `LOGOFF` at the OS/2 command prompt.
2. At the OS/2 command prompt, log on using the /L (local logon) option:

   ```
   LOGON userid /P:password /L
   ```

   Specify a user ID defined as an administrator user type at your workstation. The default administrator user ID shipped with OS/2 Warp Server is USERID. The default password is PASSWORD.
3. Add the user ID through UPM Services, specifying the user type as local administrator. For instructions, see "Adding a User" on page 264. Make sure this user ID is also defined to the domain.
4. Log on to the domain again by selecting **Logon** from UPM Services or by typing `LOGON` at the OS/2 command prompt.

Use this local administrator user ID to update database and node directories when accessing a remote database. If your workstation is configured as a database client, use this user ID to create and maintain databases on your workstation.

If you add OS/2 Warp Server to a workstation that already has a database client or database server installed, the existing user ID and group ID definitions file is overlaid with the file from the domain controller. Changes to domain user and group definitions are also copied to these workstations.

Because all the domain user and group definitions are automatically replicated to other servers in the domain when the NetLogon service starts, you should create the local administrator user ID before starting the OS/2 Warp Server software for the first time. If you start the OS/2 Warp Server software first, you must log on locally to the workstation using a user ID defined to the domain as an administrator ID. This gives you the authority to create the local administrator ID.

Granting and Revoking Operator Privileges

A user with operator privileges has certain administrative capabilities but is not a full administrator. A user may have one or more of the following types of operator privilege:

Type	Abilities
Accounts	Manage users and groups within the domain. The user can add, modify, or delete users and groups from the command line or from User Profile Management. The user cannot create or modify user accounts that have administrator or accounts operator privilege.
Print	Manage printer queues and print jobs. The user can create, modify, or delete printers or queues on servers within the domain from the command line or from Print Manager. The user can also share printer queues and manage remote jobs on shared queues.

Comm Manage serial devices. The user can share serial devices and manage remote jobs on shared serial devices from the command line.

Server Manage aliases and other shared resources and view network status. The user can create, modify, or delete aliases or other shared resources from the command line.

Operator privileges are part of the accounts database and are replicated within a domain. See the *Command Reference* for more information about operator privileges (defined in the NET USER command).

To grant operator privileges to a user, you can use the NET USER command. For example, to grant accounts operator privilege and print operator privilege to a user, type:

```
NET USER userid /OPERATOR:ACCOUNTS,PRINT
```

Note: In the previous example, the NET USER command runs at either the domain controller or in combination with the NET ADMIN command directed to the domain controller.

Updating User Information

There are two aspects to updating user information:

- Updating user information fields originally defined on the Add a New User window including:
  - User ID
  - User type (user, local administrator, or administrator)
  - Optional comments about the user ID (40 characters is the maximum)
  - Password
  - Logon authority (whether the user can log on to the domain)
- Updating group memberships for a user (adding a user to a group, deleting a user from a group)

These tasks can be done through User Profile Management.

For more information, see the following topics:

- “Updating User Information Fields”
- “Updating Group Memberships for a User” on page 268

Updating User Information Fields

Use the following procedure to update user information fields.

To update user information fields:

1. On the desktop, select **User Profile Management Services**.
2. Select **User Profile Management** from UPM Services.
3. In the User Profile Management–User Profile window, select **Manage** from the menu bar.
4. Select **Manage Users** from the Manage pull-down menu.
5. The User Profile Management–User Management window lists all users currently defined through User Profile Management.

Select the user for whom you want to update user information.

6. Select **Actions** from the menu bar.
7. Select **Update user information** from the Actions pull-down menu.
8. Complete the Update User Information window with the changed information.

Notes:

1. Passwords are validated only when they are added or changed. Therefore, if you change the status of a password from Password Optional to Password Required, but you do not change the password, it is not checked against the password limitations specified by MINPWLEN (using NET ACCOUNTS). To see the MINPWLEN restrictions, type `NET ACCOUNTS` at the OS/2 command line.

   If the status of a password is changed from Password Required to Password Optional, the password is not automatically deleted.

   To delete a password:

   a. Select **Not Required** from the Update User Information window.
   b. Select the **Change Password** option by marking the check box.
   c. Select **Delete Password**, and then select **OK** to delete the existing password.
2. Null passwords are created when a user is added and the **Password** field is left blank. If you change the status of a null password from Password Optional to Password Required, the null password remains valid.
3. For information on using the command-line interface to change password requirements, see the NET USER command in the *Command Reference*.
4. If you are changing a NET USER parameter setting of /PASSWORDREQ:Y to /PASSWORDREQ:N to cancel password requirements for a user, note that the /PASSWORDREQ:N setting does not automatically delete the user's password. After issuing NET USER *userid* /PASSWORDREQ:N, one of the following actions can be taken to delete the password. (*userid* is the user ID of the person who no longer requires a password for logon.)
   - An administrator can type `NET USER userid ""` where `""` indicates a NULL password.
   - An administrator or user can use the NET PASSWORD command to nullify the password. The password must be known by the person nullifying the password. For information on NET PASSWORD, see the *Command Reference*.

You can also view a user profile without changing it by selecting **View user profile** from the Actions pull-down menu on the User Profile Management–User Management window.

Updating Group Memberships for a User

After you have defined a user, you can select groups to which that user belongs. You can also remove a user from a group.

To update group memberships for a user:

1. On the desktop, select **User Profile Management Services**.
2. Select **User Profile Management** from UPM Services.
3. In the User Profile Management–User Profile window, select **Manage** from the menu bar.
4. Select **Manage Users** from the Manage pull-down menu.

5. The User Profile Management–User Management window lists all users currently defined through User Profile Management.

   Select the user for whom you want to update group membership.
6. Select **Actions** from the menu bar.
7. Select **Select groups for user ID** from the Actions pull-down menu.
8. The Select Groups window lists all the group IDs currently defined through User Profile Management. The groups currently assigned to the user are highlighted.

   To add a user to a group:

   Use the Spacebar to select the group ID or IDs to which the user is to belong. Select **OK**.

   To delete a user ID from a group:

   Use the Spacebar to deselect the group ID for the group from which you want to delete the user. Select **OK**.

Deleting a User

User Profile Management allows you to remove a user from the domain by deleting the user's user ID. When you delete a user ID, the following occurs:

- The user ID is erased from the list of users.
- The user ID is removed from all groups.
- The user can no longer access network resources.

The directory path and the contents of the home directory for the user ID (if one exists) and its access control profile are not deleted. These files must be deleted using the graphical user interface. For more information on deleting the home directory, see "Deleting a Home Directory" on page 57. For more information on deleting the access control profile, see "Deleting an Access Control Profile" on page 96.

Attention: Do not delete system IDs for existing servers.

To delete a user ID:

1. On the desktop, select **User Profile Management Services**.
2. Select **User Profile Management** from UPM Services.
3. In the User Profile Management–User Profile window, select **Manage** from the menu bar.
4. Select **Manage Users** from the Manage pull-down menu.
5. The User Profile Management–User Management window lists all users currently defined through User Profile Management. Select the user ID or IDs to delete from this list.
6. Select **Actions** from the menu bar.
7. Select **Erase user ID** from the Actions pull-down menu.
8. Select **Erase ID** from the Erase User ID window.

Creating a Logon Profile

You can create a *logon profile* for a user, if desired. A logon profile is a batch file containing commands that run automatically each time the user logs on.

To create a logon profile for a user, create a file with one of the following names (these file names are required):

- PROFILE.CMD for users at OS/2 clients
- PROFILE.BAT for users at DOS clients

The logon profile must be in that user's user profile subdirectory,\IBMLAN\DCDB\USERS\ *userid* for users at both OS/2 and DOS clients. If the subdirectory does not exist, create it using LAN Server Administration **Logon details** function. See "Appendix A. Directory Structure" on page 257 for more information on directory contents.

For example, for a user logging on to a DOS LAN client, the following line in the PROFILE.BAT file assigns printer queue LPT1Q on SERVER1 to local printer LPT1:

```
NET USE LPT1: \\SERVER1\LPT1Q
```

This causes the DOS LAN Services workstation to connect to the printer resource at logon.

Notes:

1. User logon profiles can only be used with user IDs that do not exceed 10 characters. This restriction also applies when adding or changing logon profiles.
2. If your network has several servers acting as backup domain controllers, make sure user logon profiles are correctly stored on each of the backup domain controllers under the correct paths. Otherwise, if there is a domain controller failure, users will not be able to access their logon profiles from the backup domain controller.
3. Currently existing environment variables cannot be permanently set through the PROFILE.CMD or PROFILE.BAT file.
4. If you log on through UPM and your PROFILE.CMD file contains an ECHO or a SAY command, you receive a NET8195 error. To avoid this error condition, log on using the command-line interface.
5. If the PROFILE.CMD file is written in REXX language, you must have the `EXIT (0)` statement at the end of the file; otherwise, a NET8195 error occurs.

Updating Logon and Desktop Application Assignments

You can define *logon assignments* for a user. Logon assignments give the user access to network resources by assigning resources to logical drives or ports each time a user logs on. The logon assignments remain in effect until changed. Both you and a user can change that user's logon assignments.

You can update logon assignments from the graphical user interface and from the command line. You also can manage a user's desktop applications from the command line.

An alias must be defined for a resource before a resource can be defined as a logon assignment. See "Chapter 6. Sharing Network Resources" on page 65for more information on defining aliases.

Managing Groups

You can create up to 250 groups in each domain. The following six additional groups already exist for each domain:

- USERS (IDs with user privileges or groups of all user IDs)
- ADMINS (administrators)
- GROUPID (default group ID)
- SERVERS (servers defined in the domain)
- LOCAL (empty group used to grant permissions to the local workstation when no one is logged on)
- GUESTS (group of guest IDs)

For more information, see the following topics:

- “Adding a Group”
- “Viewing a Group”
- “Updating a Group” on page 272
- “Deleting a Group” on page 272

Adding a Group

You can create user groups to refer to several users at the same time. On an OS/2 LAN, groups are used for access control and messaging purposes.

To add a group:

1. On the desktop, select **User Profile Management Services**.
2. Select **User Profile Management** from UPM Services.
3. In the User Profile Management–User Profile window, select **Manage** from the menu bar.
4. Select **Manage Groups** from the Manage pull-down menu.
5. The User Profile Management–Group Management window lists all groups currently defined through User Profile Management. Select **New** from this list.
6. Select **Add a new group** from the Actions pull-down.
7. Complete the Add a New Group window. Specify the group ID and any optional comments. Select the user IDs to belong to the group. To confirm or update the new group, see “Updating a Group” on page 272.

Viewing a Group

You can view the list of users in a group after the group is created. This task can be done through User Profile Management.

To view a group:

1. On the desktop, select **User Profile Management Services**.
2. Select **User Profile Management** from UPM Services.
3. In the User Profile Management–User Profile window, select **Manage** from the menu bar.
4. Select **Manage Groups** from the Manage pull-down menu.

5. The User Profile Management–Group Management window lists all groups currently defined through User Profile Management. Select the group to view from this list. You can only view one group at a time.
6. Select **Actions** from the menu bar.
7. Select **View group** from the Actions pull-down menu.

   The View Group window displays the users in the selected group.

Updating a Group

You can change the list of users in a group after the group is created. This task can be done through User Profile Management.

To update a group:

1. On the desktop, select **User Profile Management Services**.
2. Select **User Profile Management** from UPM Services.
3. In the User Profile Management–User Profile window, select **Manage** from the menu bar.
4. Select **Manage Groups** from the Manage pull-down menu.
5. The User Profile Management–Group Management window lists all groups currently defined through User Profile Management. Select the group to update from this list. You can only update one group at a time.
6. Select **Actions** from the menu bar.
7. Select **Update group** from the Actions pull-down menu.
8. Complete the Update Group window with the changed information. You can add new users to the group or remove users from the group. The users currently assigned to the group are highlighted.

Deleting a Group

Besides deleting individual users and removing users from groups, you can remove a group from the domain. Users in the deleted group no longer have permissions that may have been granted to them through membership in the group. However, deleting a group does not affect the individual user IDs and their associated user profiles.

This task is done through User Profile Management.

To delete a group:

1. On the desktop, select **User Profile Management Services**.
2. Select **User Profile Management** from UPM Services.
3. In the User Profile Management–User Profile window, select **Manage** from the menu bar.
4. Select **Manage Groups** from the Manage pull-down menu.
5. The User Profile Management–Group Management window lists all groups currently defined through User Profile Management. Select the group or groups to delete from this list.
6. Select **Actions** from the menu bar.
7. Select **Erase group** from the Actions pull-down menu.
8. Select **Erase ID** in the Erase Group ID window.

Attention: Do not delete the groups named SERVERS or USERS.

Appendix C. OS/2 Warp Server Interoperability

This appendix identifies how the various versions of OS/2 Warp Server, LAN Server and PCLP work together. You should read this appendix if you will have servers running various versions of OS/2 Warp Server and LAN Server software in your network. You also should read this appendix if you will use both PCLP and OS/2 Warp Server in your network.

Introduction

Table 3 on page 274 describes the access capabilities of various IBM LAN clients to resources on IBM LAN server domains. The following three areas are described:

- Logging on to a domain
- Administering a domain
- Accessing resources across domains

The IBM LAN server domains described are:

- PCLP 1.31 (or later)
- OS/2 LAN server 1.3
- OS/2 LAN server 2.0
- OS/2 LAN Server 3.0
- OS/2 LAN Server 4.0
- OS/2 LAN Server 5.0
- OS/2 Warp Server for e-business

The IBM LAN clients described are:

- PCLP 1.31 (or later) Base Services Requester (also requires IBMLAN Support Program)
- PCLP 1.31 (or later) Extended Services Requester (also requires IBM LAN Support Program)
- OS/2 LAN Requester shipped with OS/2 Extended Edition 1.3
- OS/2 LAN Requester shipped with LAN Server 2.0 and LAN Server
- DOS LAN Services shipped with OS/2 LAN Server 1.3, 2.0, and 3.0, and OS/2 Warp Server for e-business (also requires IBM LAN Support Program)
- LAN Enabler 2.0 (includes OS/2 LAN Requester and DOS LAN Services)

For more information, see the following topics:

- “File and Print Sharing Server Client/Server Interoperability”
- “Interoperability with Windows for Workgroup Clients” on page 278

File and Print Sharing Server Client/Server Interoperability

Table 3 on page 274 illustrates the capabilities of various client products when used with various server services. The table distinguishes the following capabilities:

Resource access
Determines connectivity to file, print, and serial device resources.

Logon Services
Determine validation of domain logon requests.

Domain awareness Determines the ability to connect to resources by alias, to launch network applications, and to use other centrally administered domain services.

Administrative capabilities Determine the ability to administer servers and domains.

Only LAN Server servers can participate as full servers within a LAN Server domain. Users access resources on other servers, either by referring to the server and its resource by name, using a Universal Naming Convention (UNC) name such as\\SERVER1\C-DRIVE, or by connecting to a *cross-domain alias*. A cross-domain alias refers to a server outside the domain and is created like a normal alias, except that the server is not defined within the domain.

A user logged on to an OS/2 or DOS LAN Requester can connect to resources on any number of servers, whether or not the servers are within the user's domain. However, when a server outside the domain has user-level security, the user must either be defined on that server with the same password as in the logon domain, or access the resource as a guest, assuming that the guest account (usually GUEST) has access to the resource.

When passwords are assigned to shares (share-level security), the NET USE command must be used so that the password can be specified on the command.

Table 3. File and Print Sharing Server Client/Server Interoperability

Clients	**Servers**							
	PCLP 1.31 or later (Base Services) [7]	**PCLP 1.31 or later (ES)** [7]	**LAN Server 2.0, 3.0 or 4.0**	**OS/2 Warp Server 4.0 File and Print Sharing**	**Microsoft LAN Manager; Windows NT and NTAS; Windows for Workgroups**	**LAN Server 4.0; OS/2 Warp Server 4.0; Peer Services for OS/2**	**LAN Server 4.0; OS/2 Warp Server 4.0; Peer Services for DOS**	**Peer for OS/2 from Warp Connect**
PCLP 1.31 or later (Base Services) [7]	R	R [1], L [2]	R [1], L [2]	R [1], L [2]	R [1]	R [1,3]	R [1,3]	R
PCLP 1.31 or later (ES) [7]	R	L,A						
OS/2 LAN Requester (shipped with LAN Server 2.0, 3.0 or 4.0, LAN Enabler 2.0, or Warp Connect)	R	R	R,L,D,A	R,L,D,A	R	R [3], A [10]	R [1,3]	R,A [10]

Table 3. File and Print Sharing Server Client/Server Interoperability (continued)

Clients	Servers							
	PCLP 1.31 or later (Base Services) (7)	**PCLP 1.31 or later (ES) (7)**	**LAN Server 2.0, 3.0 or 4.0**	**OS/2 Warp Server 4.0 File and Print Sharing**	**Microsoft LAN Manager; Windows NT and NTAS; Windows for Workgroups**	**LAN Server 4.0; OS/2 Warp Server 4.0; Peer Services for OS/2**	**LAN Server 4.0; OS/2 Warp Server 4.0; Peer Services for DOS**	**Peer for OS/2 from Warp Connect**
OS/2 LAN Requester (shipped with OS/2 Warp Server 4.0 and OS/2 Warp Server for e-business)	R	R	R,L,D,A	R,L,D,A	R	R (3), A 10	R (1,3)	R,A (10)
DOS LAN Requester (shipped with LAN Server 2.0, 3.0 or 4.0)	R	R	R,L,D,A (4)	R,L,D,A (4)	R	R (3), A (10)	R (1,3)	R,A (10)
DOS LAN Services (shipped with OS/2 Warp Server 4.0, LAN Server 4.0, and OS/2 Warp Server for e-business)	R	R	R,L,D,A (5)	R,L,D,A (5)	R	R (3),A (10)	R (1,3)	R,A (10)
Windows 95 Client (shipped with OS/2 Warp Server 4.0)	R	R	R,L,D,A (5)	R,L,D,A (5)	R	R (3),A (10)	R (1,3)	R,A (10)

Table 3. File and Print Sharing Server Client/Server Interoperability (continued)

Clients	**Servers**							
	PCLP 1.31 or later (Base Services) (7)	**PCLP 1.31 or later (ES) (7)**	**LAN Server 2.0, 3.0 or 4.0**	**OS/2 Warp Server 4.0 File and Print Sharing**	**Microsoft LAN Manager; Windows NT and NTAS; Windows for Workgroups**	**LAN Server 4.0; OS/2 Warp Server 4.0; Peer Services for OS/2**	**LAN Server 4.0; OS/2 Warp Server 4.0; Peer Services for DOS**	**Peer for OS/2 from Warp Connect**
Windows 95 Client with IBM Network Clients for Windows 95 (shipped with OS/2 Warp Server for e-business	R	R	R,L,D,A (5)	R,L,D,A (5)	R	R (3),A (10)	R (1,3)	R,A (10)
Microsoft LAN Manager	R	R	R,L,A (8)	R,L,A (8)		R,A (8)	R	R
Microsoft NT or NTAS	R	R	R,A (8)	R,A (8)		R,A (8)	R	R
Microsoft NT with IBM Primary Logon Client for Windows NT (shipped with OS/2 Warp Server for e-business)	R	R	R,A (8)	R,A (8)		R,A (8)	R	R
Microsoft Windows for Workgroups (9)	R	R	R,L	R,L		R	R	R
Workgroup Connection for DOS	R	R	R,L	R,L		R	R	R,L

Abbreviations:

- R = access to shared resources (file, print, serial)
- L = domain logon capability

- D = Domain Services (aliases, application definitions, etc.)
- A = administrative capabilities
- ES = Extended Services
- PCLP = PCLP

Notes:

1. Remote access to serial devices is not supported.
2. The network administrator defines a user ID that matches the machine name of the PCLP Base Services workstation. When the workstation issues a NET USE command, the machine name is validated against the defined user IDs.
3. Peer Services for DOS and OS/2 are limited to sharing with one client at a time (single session).
4. Administrative capability from the DOS LAN Requester client is available only from the LAN Server application programming interface (API). A large number of categories that support remote network administration are supported. For more information, refer to the *Programming Guide and Reference*.
5. In addition to the API support described in the previous note, DOS LAN Services for LAN Server 4.0 includes the NET ADMIN command, which allows full command line administration of LAN Server.
6. PCLP and Microsoft servers cannot be defined within a LAN Server domain; access to those resources are cross-domain.
7. PCLP is available on SBCS systems only.
8. Partial administration function only.
9. Domain Services can be added by installing the DLS requester shipped with LAN Server 4.0.
10. Command line administration via NET ADMIN only.

Administration of LAN Server 2.0 or 3.0 Users and Aliases from the LAN Server Administrator GUI

There are some restrictions when using the LAN Server Administration GUI to administer domains running earlier levels of LAN Server:

- A user account running in a LAN Server 2.0 or 3.0 domain cannot be modified or deleted once it’s created from the LAN Server Administration GUI. If you are using the GUI to update or delete a user in a LAN Server 2.0 or 3.0 domain, the NET.ACC file on the 2.0 or 3.0 domain cannot be updated and no error message is displayed.
- An alias maintained in a LAN Server 2.0 or 3.0 domain cannot be changed after its initial creation from the LAN Server Administration GUI. If you use the GUI to update the alias, the DCDB on the 2.0 or 3.0 domain is not updated and no error message will be displayed.

Interoperability with Windows for Workgroup Clients

IBM LAN Server 5.0 and Microsoft Windows for Workgroup (3.1 or 3.11) are generally compatible and can interoperate to communicate with each other across a LAN. This section describes some of the considerations when operating in this environment. This section focuses on Windows for Workgroups operating with its native client and peer server and connecting with an OS/2 LAN Server client, Peer Services, and server across a LAN.

For more information, see the following topics:

- “Transports”
- “Logging On”
- “Browsing Domains and Servers”
- “File Resources” on page 279
- “Printer Resources” on page 279

Transports

The IBM and Microsoft implementation of NetBIOS transports are compatible with each other and can communicate well across a network. You must, of course, install hardware LAN adapters and the correct drivers for those adapters on both the Windows for Workgroups and the LAN Server workstations. The adapter types and drivers supported in the two environments are different, and you must ensure that your choice of adapter is compatible with each environment.

Logging On

Windows for Workgroups clients can log on to a LAN Server domain. Configure the Window for Workgroups clients with its logon workgroup name equivalent to the LAN Server domain name. You can do this through the Control Panel Network icon.

Home directories, logon assignments, network applications, and PROFILE.BAT are not supported from Windows for Workgroups clients.

Browsing Domains and Servers

Windows for Workgroups has adopted a different browsing scheme than OS/2 LAN Server. However, the two browsing schemes are interoperable with the following constraints. Windows for Workgroups clients can browse LAN Server domains and servers. If you have logged on to a LAN Server domain, that domain’s server will be visible to you when you browse using the File Manager or Print Manager. All other Windows for Workgroups peer servers in other domains should also be visible to you.

To browse a LAN Server domain that you have not logged on to, bring up the File Manager’s Connect Network Driver dialog box and type a known server name located in that domain in the **Path** field. (for example, \\OS2SRV), and then press Enter. Windows for Workgroups will begin browsing that server’s domain. When finished, the domain’s shared directory aliases are displayed. To display peer client shared directory aliases, repeat the above steps using a client name.

LAN Server clients can browse resources shared from Windows for Workgroups workstations from the command line interface. On the Windows for Workgroups workstations, you can add a parameter to the\WINDOWS\SYSTEM.INI file to allow the client to browse resources. In the [network] section of the SYSTEM.INI file, add the following line:

```
lmannounce=yes
```

This makes the Windows for Workgroups server visible to the LAN Server client which is browsing the same domain. If you do not add this parameter, you will have to specify the name of the Windows for Workgroups server when you connect to resources.

File Resources

Windows for Workgroups clients can use LAN Server file resources, as long as the files and directories conform to the DOS FAT 8.3 naming convention. Long file names are not visible to Windows for Workgroups clients.

To connect to a LAN Server file alias, you must specify the server name and the alias name, not just the alias name. Windows for Workgroups does not support single system image connections.

LAN Server clients can use Windows for Workgroups file resources, except that 32-bit OS/2 applications cannot use the DosFindFirst and DosFindNext APIs. This means that OS/2 desktop Drive objects cannot be used to view Windows for Workgroups file resources, nor can the OS/2 desktop Network folder be used. Use a DOS or OS/2 window to view file names.

Printer Resources

Windows for Workgroups can use LAN Server printer resources as long as connections are made using the server name and printer queue name (for example, \\SERVER1\PRINTER1). The Windows for Workgroups Print Manager can be used to view and manipulate LAN Server printer queues.

To connect to a LAN Server printer alias, open the Windows for Workgroups Print Manager and select **Connect Network Printer**.

Appendix D. DHCP RIPL Bootstrap Messages

During the first phase of the bootup process, no operating system or font services are available, so error messages are displayed through BIOS functions. Only the characters supported by machine ROM BIOS (code page 437) can be displayed. These error messages and the associated help for them are described below.

```
BPD0000I: The file identified on the next line displayed cannot be found.
Help: Make sure the identified file exists on the server in the path specified.

BPD0001I: The DHCP boot cannot continue.
Help: Fatal error. DHCP boot client cannot continue its boot process.

BPD0002I: No response from a DHCP/BOOTP server.
Help: Check that the network is functioning. Make sure the client can reach the DHCP
server and remote IPL server. Ensure that DHCP and BINL server services are started and
client can reach these servers.

BPD0003I: Not enough memory is available to DHCP boot this machine.
Help: DHCP boot client machine needs at least 16 MB RAM.

BPD0004I: TFTP downloading of files started.

BPD0005I: TFTP downloading of files completed.

BPD0010I: Invalid file handle.
Help: File might not exist. Make sure that the specified file is in BPCOMMON and make sure
that the file exists on the server.

BPD0011I: No machine name created at WorkSpace On-Demand server.
Help: Create a machine (client) definition for this machine LAN address on WorkSpace On-Demand
server.

BPD0012I: The buffer address passed by OS/2 is invalid.
Help: Critical OS/2 error. Verify the OS/2 image installed on the WorkSpace On-Demand server's
client tree is not corrupted.

BPD0013I: The read request is beyond the end of file.
Help: Critical OS/2 error. Verify the OS/2 image installed on the WorkSpace On-Demand server's
client tree is not corrupted.

BPD0014I: The file data copy from high to low memory failed.
Help: This might be causing due to int 15 function provided by the BIOS in the system.
Flash the BIOS if new level BIOS is available.

BPD0020I: Invalid file handle.
Help: Internal OS/2 error. If the system boots properly, you may ignore this message,
because the system recovered from this error.  If the system fails, contact IBM.

BPD0021I: Not enough memory is available to DHCP boot this machine.
Help: DHCP boot client machine needs at least 16 MB RAM. If this condition is already
met then it could be an Internal File System error. Contact IBM.

BPD0022I: MFSD can not simultaneously open more than one file.
Help: Critical OS/2 error. Verify the OS/2 image installed on the WorkSpace On-Demand
server's client tree is not corrupted.

BPD0023I: The read request is beyond the end of file.
Help: Internal OS/2 error. If the system boots properly, you may ignore this message,
because the system recovered from this error. If the system fails then verify that the
OS/2 image installed on the WorkSpace On-Demand server's client tree is not corrupted.

BPD0024I: Unable to initialize MFSD data structures.
Help: Critical OS/2 error. Verify the OS/2 image installed on the WorkSpace On-Demand
server's client tree is not corrupted.

BPD0025I: Error handling FIT file.
Help: FIT file size is greater than 64K. Reduce the size of the fit file and reboot
the client machine.

BPD0026I: Network access denied.
Help: A program has attempted to access a file that it does not have permission to
access. If the system functions properly, you may ignore this message. Otherwise a
program is probably attempting to write or replace a file to which it has only read
or execute authority.
```

Appendix E. Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the information. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this information at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Department LZKS
11400 Burnet Road
Austin, TX 78758
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM’s future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM’s suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, or other countries, or both:

AT
Extended Services
First Failure Support Technology/2
FFST/2
IBM
LANStreamer
Micro Channel
OS/2
Presentation Manager
SP
WIN-OS/2

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States and/or other countries.

Other company, product, and service names may be trademarks or service marks of others.

Index