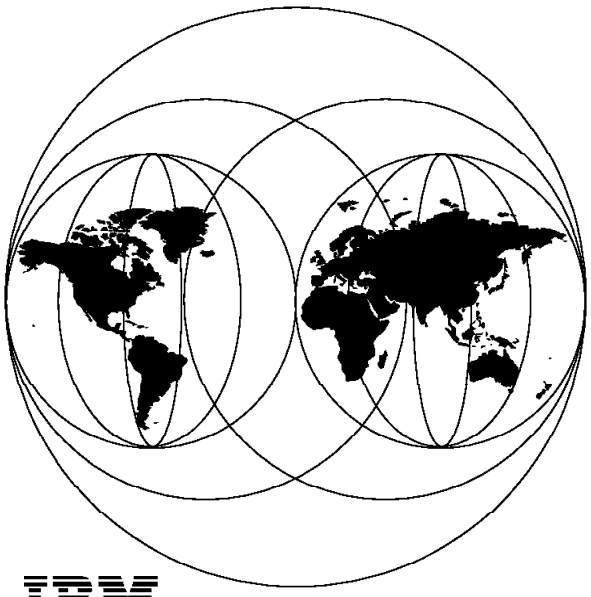
SG24-4880-00

ADSM Client Disaster Recovery: Bare Metal Restore

April 1997



IBM
International Technical Support Organization
San Jose Center

SG24-4880-00

International Technical Support Organization

ADSM Client Disaster Recovery: Bare Metal Restore

April 1997

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix C, “Special Notices” on page 281.

First Edition (April 1997)

This edition applies to Versions 1 and 2 of ADSM for AIX, Program Numbers 5765-203 and 5765-564; Versions 1 and 2 of ADSM for MVS, Program Numbers 5748-020 and 5655-119; ADSM for VM, Program Number 5648-020; ADSM for OS/2, Program Number 5622-112; ADSM for OS/400, Program Numbers 5737-197 for OS/400 Version 2 Release 3, 5763-SV1 for OS/400 Version 3 Releases 0.5 and 1, and 5716-SV for OS/400 Version 3 Release 6; ADSM for VSE/ESA, Program Number 5686-073; ADSM for HP-UX, Part Number 14H0260 (5871-AAA); and ADSM for SUN Solaris, Part Number 28H2189 (5871-AAA).

Comments may be addressed to:
IBM Corporation, International Technical Support Organization
Department QXXE Building 80-E2
650 Harry Road
San Jose, California 95120-6099

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Contents

Figures

Preface

This redbook describes how to use ADSTAR Distributed Storage Manager (ADSM) to recover from the complete loss of an ADSM client system. Recovery may be required because of a disaster, such as a fire or flood, or a simple hard disk failure that prevents a system from booting. We describe various techniques including bootable recovery, recovery using remote distribution tools, and recovery using peer services to recover ADSM clients on the OS/2, Windows, Novell NetWare, and AIX platforms.

We wrote this redbook to help fill an information gap. Much has been written about the recovery of the ADSM server environment. Any discussion of ADSM client environment recovery typically begins at the point when ADSM data file restoration is about to start. This redbook focuses on the recovery of the ADSM client environment from the bare metal up, including the operating system and communications software that have to be in place for the ADSM client to begin its restoration work. We call this recovery the bare metal restore of ADSM clients.

This redbook is written for ADSM administrators who are concerned with creating a comprehensive disaster recovery plan that includes not only the ADSM server environment but also the restoration of the ADSM client environment from the bare metal up.

We describe actual examples of the bare metal restore of ADSM clients on the OS/2, Windows, Novell NetWare and AIX platforms. We also discuss how ADSM′s Disaster Recovery Manager (DRM) feature can be used in the context of ADSM client recovery.

Some knowledge of ADSM and the corresponding client operating system (OS/2, Windows, Novell NetWare, or AIX) is assumed.

We assume that most readers will already be using ADSM and that they will be looking for specific help on the bare metal restore of one or more platforms. Accordingly, the book consists of a basic introduction to ADSM and discrete chapters that give procedures for those platforms. In some cases the procedures are very similar. To make the book easy to use there is some repetition between chapters. If you are reading from cover to cover, we apologize for this.

The Team That Wrote This Redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization San Jose Center.

The project was designed and managed by **Patrick Randall**. Pat is a Distributed Storage Specialist at the IBM International Technical Support Organization, San Jose Center. He has written five redbooks on ADSM, teaches IBM classes worldwide on all areas of distributed storage, and is a consultant in disaster and business recovery. Before joining the ITSO in July 1996, Pat worked in IBM UK's Business Recovery Services as a Solutions Architect.

The authors of this book are:

Rene Aguilar is an S/390 Systems Engineer for IBM Chile. He has 16 years of experience in S/390 hardware and software, and just over a year's experience with ADSM. Rene has taught many customer courses. He holds a degree in electrical engineering from the University of Santiago.

Dave Armes is an AIX Support Specialist for IBM UK. He has been with IBM for two years working with ADSM in the AIX environment. Dave has a degree in applied physics from Brunel University and is a qualified AIX Support Professional.

Klaus Dilper is a customer from the University of Karlsruhe, a very large ADSM installation and reference account. Klaus has been involved with the ADSM product since its inception. He has more than 12 years of experience with the S/390 platform and two years of experience with AIX. Klaus has presented talks on ADSM at various conferences, including SHARE/GUIDE Europe, and is a frequent contributor to the ADSM forums.

Sandy Fabbi is an ADSM Specialist for IBM Canada. She has nine years of experience in data processing and disaster recovery and one year of experience with ADSM. She holds a degree in computer science from the University of Toronto.

Fu Chee Tai is an S/390 Advisory Systems Engineer for IBM Singapore. He has 16 years of experience in S/390 hardware and software and about four months of experience with ADSM. Fu has a degree in physics from the Nanyang University and a degree in communications engineering from London Imperial College.

Thanks to the following people for their invaluable contributions to this project:

Maggie Cutler
Editor
International Technical Support Organization, San Jose Center

Cybelle Beaulieu
International Technical Support Organization, San Jose Center

Paul Zarnowski
Cornell

Jerry Lawson
ITT Hartford

Cyndie Behrens
International Technical Support Organization, San Jose Center

Tim Mortimer
International Technical Support Organization, San Jose Center

Pete Tanenhaus
ADSM Client Development, San Jose

Kenneth Morse
IBM Washington Systems Center

Jim Smith
IBM San Jose ADSM Programming Lab

Alan Tippett
International Technical Support Organization, San Jose Center

Dave Wray
International Technical Support Organization, San Jose Center

Comments Welcome

We want our redbooks to be as helpful as possible. Should you have any comments about this or other redbooks, please send us a note at the following address:

redbook@vnet.ibm.com

Your comments are important to us!

Chapter 1. Introduction to ADSM

This chapter provides a brief overview of Adstar Distributed Storage Manager (ADSM). We look at its components and describe key functions such as scheduling and policy management. We conclude with a discussion of the Disaster Recovery Manager (DRM) feature and its possible uses during bare metal restores of ADSM clients.

1.1 What Is ADSM?

ADSM, IBM′s solution to enterprisewide distributed storage management, is a client/server program product. It provides highly automated, centrally scheduled, network-based backup and archive functions for workstations and local area network (LAN) file servers. ADSM supports a wide variety of IBM and non-IBM clients and servers (see Figure 1 on page 2) and addresses the need for customer asset protection and data availability for distributed environments.[1]

[1] The material in this chapter is summarized from the following sources:

Chapter 1 of *Using ADSM to Back up Databases*, SG24-4335.

Chapters 1 through 5 of *ADSM for AIX: Advanced Topics*, SG24-4601.

Chapter 1 of *Disaster Recovery Manager Administrator′s Guide and Reference*, GC35-0238.

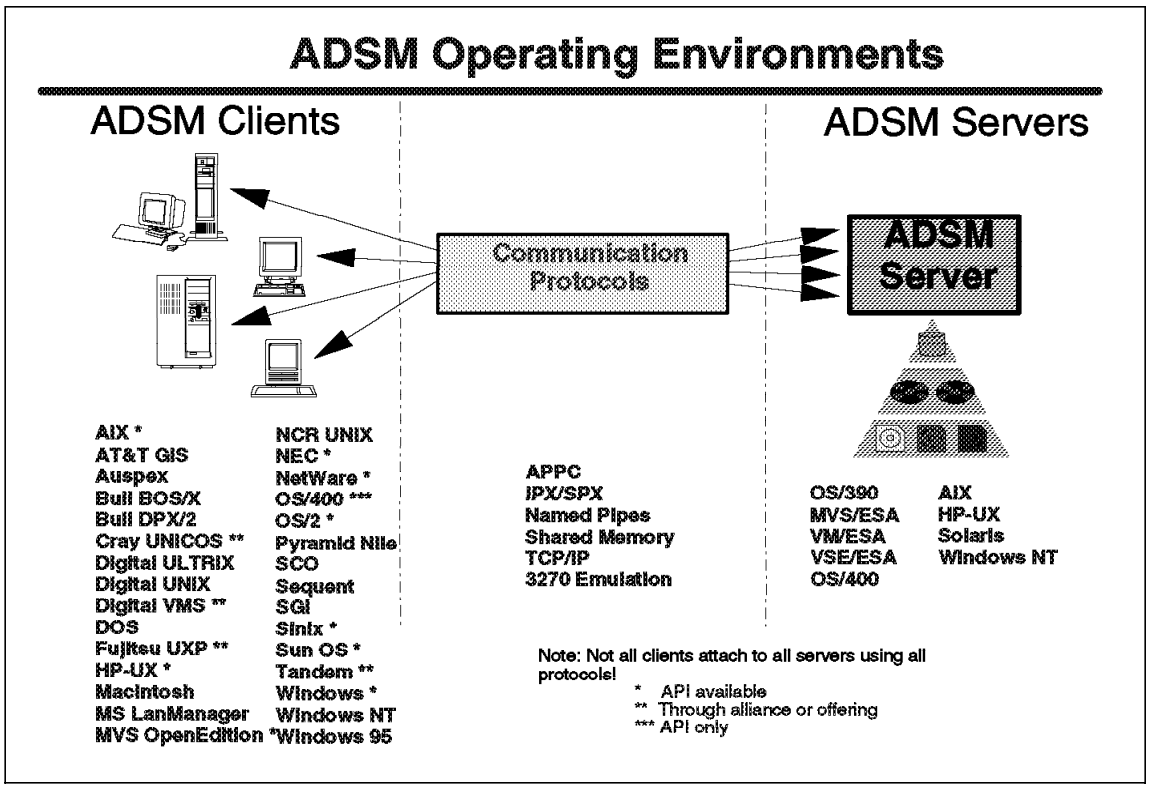


Figure 1. ADSM Platforms

1.2 Main Components

In this section we look at the main components of ADSM—the backup/archive client, administrative client, and server, as shown in Figure 2 on page 3—and briefly review the application client.

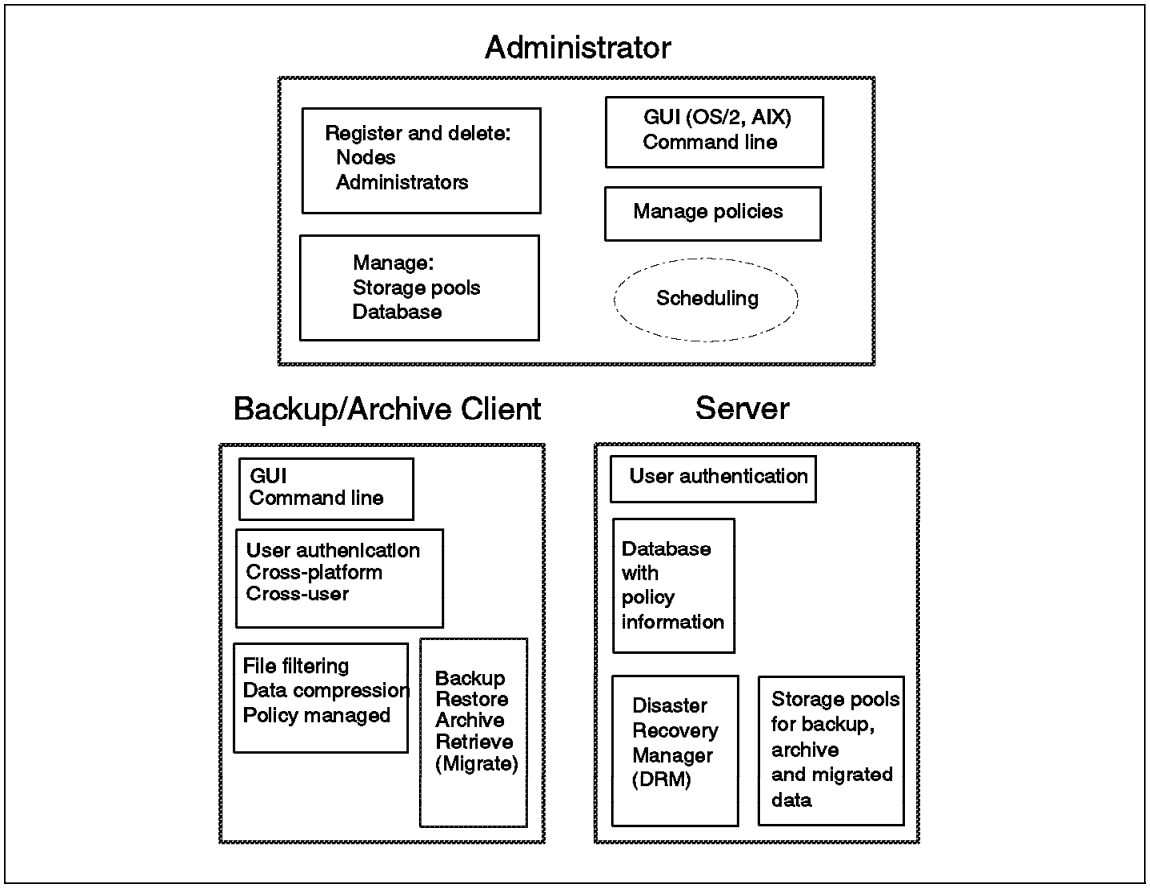


Figure 2. ADSM Storage Management Components

1.2.1 Backup/Archive Client

The backup/archive client runs on the workstation and, depending on the platform, provides both a graphical user interface (GUI) and command line interface (CLI). Although all clients are similar, each has the look and feel of the platform on which it runs. Thus users can back up or restore files, using an interface with which they are familiar.

The main function of ADSM is backup and restore. You can back up all of your files (full), specific files (selective), or only those files that have changed since your last backup (incremental). You can specifically include or exclude certain files from being backed up.

The file compression provided on the client platforms reduces network traffic and the amount of storage required on the server to store the files.

ADSM′s cross-user restore and cross-platform restore provide you with significant flexibility. Cross-user restore enables you to authorize someone else to restore your files. Cross-platform restore enables you to restore your file on a platform different from the platform on which it was backed up. For example, you could back up your file from a DOS workstation but then restore it to an OS/2 workstation. Cross-platform restore can be extremely useful when you migrate to new workstation platforms, or even if you happen to work at a different office one day that has different workstations. You will still have access to the data you backed up!

A separate archive/retrieve function is also part of ADSM. This function provides a way for you to store files that you may not use but have to retain for long-term storage. Archive is also useful as a way of reducing the disk space on your workstation. You can archive files for long-term storage and erase the original files from your workstation to create room for more active files and applications.

1.2.2 Administrative Client

As shown in Figure 3 on page 5, the ADSM administrative client has functions that allow an administrator to control and monitor server activity, define storage management policies for workstation files, and set up schedules to provide backup and archive services.

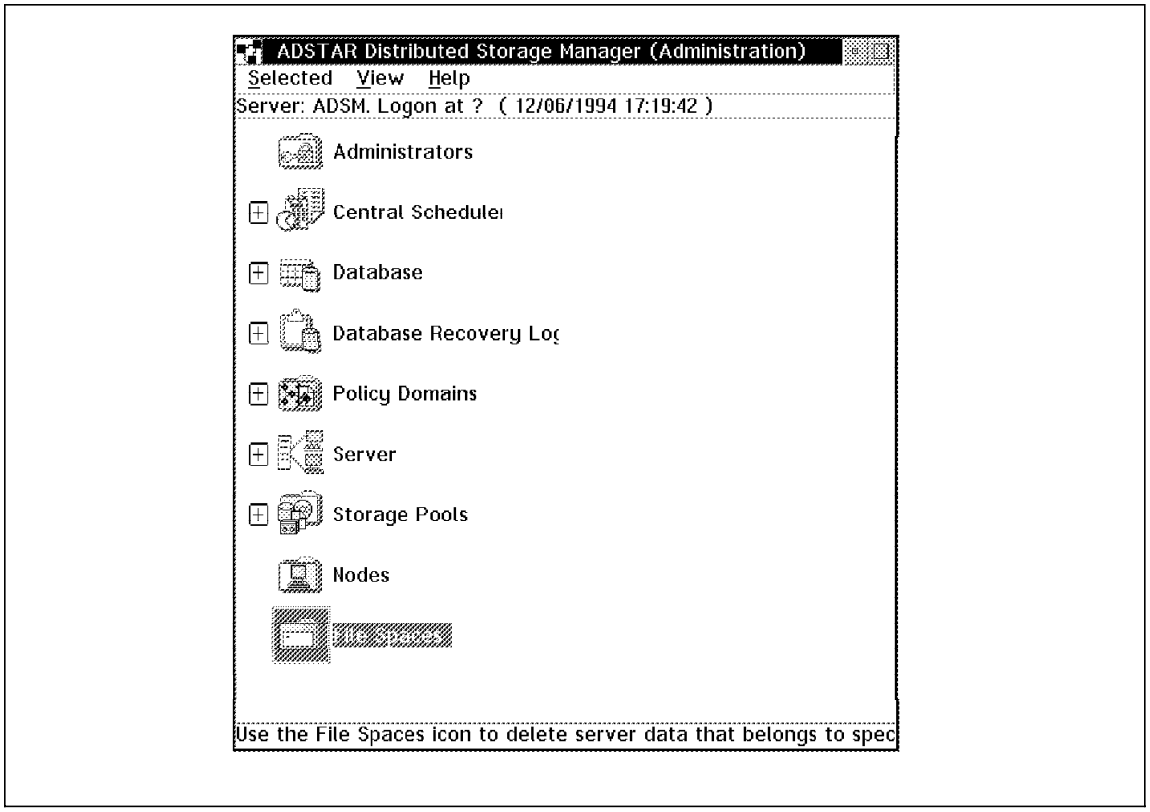


Figure 3. ADSM Administrative Client GUI

An administrative client is a program that enables administrators to control and monitor the server through administrative commands. The administrative program can be installed on a programmable workstation (PWS), personal computer, or mainframe. An administrative client passes commands through an administrative command line. In some cases, a GUI has been added to the administrative client code.

ADSM provides a hierarchical structure to the authority you can grant an administrator. Thus you can establish as flexible an administration scheme as you would like while still providing control over your system. The ADSM administrator with overall authority is called the *system administrator*. Other administrators are called *policy, storage, operator*, or *analyst administrators*, depending on which part of the system they control. Their administrative tasks are separated into logical categories, such as controlling management policies, storage pools and databases, operation of the server, and analysis of certain server events.

Dividing up the administrative authority according to logical categories of tasks is not the only way of granting authority. You can also divide up the administrative authority by organization. You can give the logical categories of authority to a department, but only for the data that belongs to that department. For example, you can give a department policy and storage authority for the policy domain and storage pools that it owns.

1.2.3 Server

The server component provides storage resources and services for the backup/archive clients. Users can back up or archive their files onto server storage resources such as disk, tape, or optical devices that the ADSM server policy manages and monitors. .

Figure 4 shows the two key components of the ADSM server: the storage pools where the client files are actually stored, and the database that serves as an inventory or index to the client files within the storage pools. The database consists of the database space and the recovery log. The recovery log keeps track of all changes made to the database.

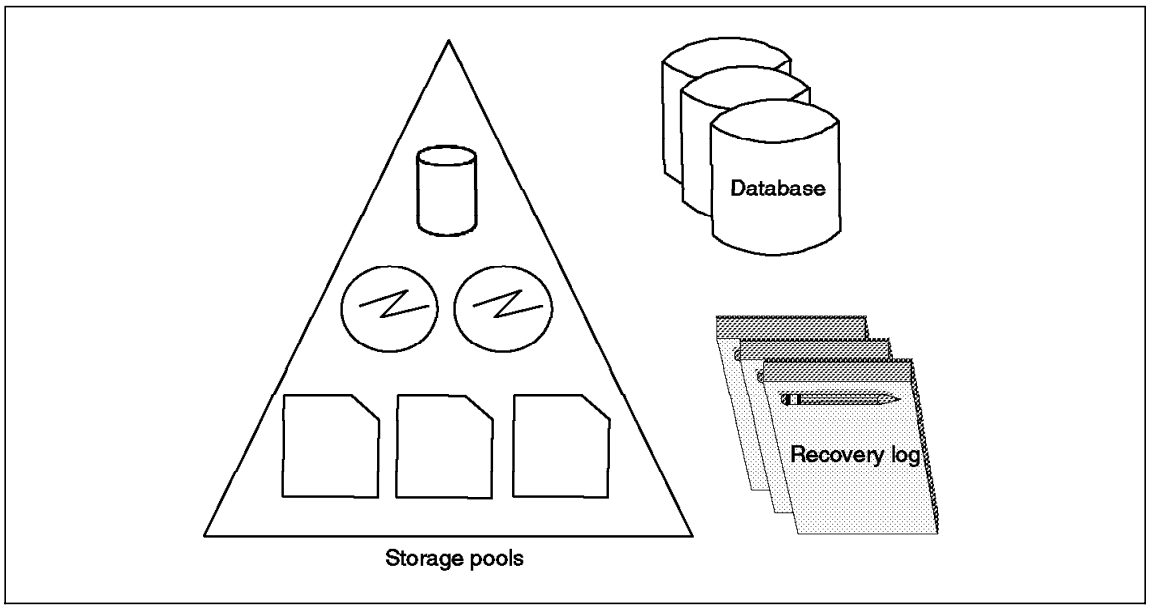


Figure 4. ADSM Server Components

The storage pools contain the client files that have been backed up, archived, or migrated.

You can use a hierarchy of storage media to define the storage pools. The pools can contain disk storage, optical devices, and tape devices. Each

ADSM server platform supports a different set of storage media, so please verify the devices that are supported in your environment.

You can move data automatically through the storage hierarchy onto less expensive media with ADSM′s migration function. Additional management functions are provided, such as reclamation and collocation for tape management.

The ADSM server is multitasking, so multiple clients can back up data concurrently.

The ADSM database is the heart of the server. It is critical to the operation of ADSM because it contains file location information as well as policy and scheduling information. The following information is stored in the database:

- Information about registered client nodes
- Policies assigned to those client nodes
- Schedules and their association with client nodes
- Event records, such as whether a schedule successfully completed
- The activity log that contains the messages generated by the server
- Information about ADSM volumes
- The data storage inventory, that is, the information used to locate files that reside in storage pools
- Disaster recovery information (if the DRM feature is installed on the ADSM server. DRM is currently supported on the AIX and MVS ADSM server platforms.)

The database has all of the features associated with a database management system. Because the database is critical, many features are built into ADSM to help maintain the availability, integrity, and performance of the database. Two of these features are the recovery log and mirroring.

A recovery log is used to help maintain the integrity of the database. It keeps track of all changes made to the database, so that if a system outage were to occur, a record of the changes would be available in the log. When a change to the database occurs, the recovery log is updated with some transaction information before the database is updated. Thus uncommitted transactions can be rolled back during recovery so that the database remains consistent.

Mirroring is the process of writing the same data to multiple storage devices at the same time. The administrator can configure the server so that up to three copies of the database and recovery logs are maintained at all times.

This mirroring capability provides nondisruptive and immediate recovery from physical failures on database and recovery log volumes.

If a mirrored volume encounters a media failure, the server automatically places the failing volume offline and continues database operations, using the other mirrored copies. Once the failed disk is replaced and made available to the server, it is automatically synchronized with the intact copies.

The mirroring facility improves database performance. The mirrored copies are treated equally; there is no concept of primary copy and alternate copies. Therefore, the server reads from the database copy that is on the device with the best response time.

Another server function, export/import, creates a self-describing copy of specified server information. Information that can be exported includes:

- Administrator information
- Client node definitions
- Policy information
- Backup and archive data

Export/import is useful for migration and conversion, workload balancing, and cloning of information.

ADSM provides extensive ADSM server database and storage pool backup facilities. Incremental backups are provided as well as a mechanism for offsite backups to aid in disaster recovery.

1.2.4 Application Client

The application client is a software application that runs on a workstation and uses the ADSM application programming interface (API) to back up, archive, restore, or retrieve objects from an ADSM server.

The application client program enables other IBM and non-IBM products to use the storage management services of ADSM. The application client allows applications to back up or archive valuable data in any format that an application programmer specifies.

The number of ways of using the API is unlimited. You can use it to improve the handling of nonfile data in the enterprise, such as databases or image volumes. You could, for example, provide extensions to the existing ADSM backup and restore functions to meet your user′s needs or write a virtual tape device driver so that other applications can use ADSM transparently.

The API is available for the C programming language.

1.3 Functions

In this section we look at the ADSM backup and restore, archive and retrieve, central scheduling, and policy management functions. Then we concentrate on the disaster recovery features and functions of ADSM.

1.3.1 Backup and Restore

The backup process creates a copy of a client file on the ADSM server. The backup process also backs up the directory in which the file resides.

Incremental backup sends to the server the files that have changed since the last backup. The first time an incremental is done, all files are sent to the ADSM server. This is a full backup. ADSM determines that a file has changed if any of the following has changed: file size, date and/or time stamp, file owner, file group, file permission, or attribute change time.

Selective backup specifies which files a user wants to back up. A selective backup can consist of a single file, or a user can select a directory or sub-directory tree to back up. Because wildcards are allowed in the specification, there is great flexibility in file selection.

The files are backed up according to policies that the administrator has predefined. The policies define, for example, how many backup versions should be retained in the ADSM storage pools, how long to retain those versions, and whether to back up files that are in use.

Restore is the process of copying a backup version from the server to the client. This process is system assisted; that is, the system performs the restore for the user. The user does not have to call the ADSM administrator to request restoration of the file.

1.3.2 Archive and Retrieve

The archive process creates a copy of a client file on the ADSM server. As with backup, archived files are managed on the basis of policies; however, the archive function does not have a concept of versioning. You can archive multiple versions of a file by invoking the archive function multiple times. In other words, each archived copy is treated as a separate file, not as multiple versions of a single file.

A user can save a description of an archived file so that it will be easy to retrieve the file if multiple files are archived with the same file name.

The key difference between backing up a file and archiving a file is that the user can erase the original file after archiving it. The archived version is expected to be retained for a long time. Erasing the original file does not affect the retention period for the archived file.

1.3.3 Central Scheduling

As shown in Figure 5 on page 11, the ADSM central scheduling facility automates the initiation of client backup, archive, restore, and retrieve, as well as ADSM server administrative operations. It also can schedule any client operating system command and ADSM client macros. New clients can be easily associated with schedules in a nondisruptive manner. The central scheduler consists of client and server processes that cooperate to execute the scheduled functions. Thus ADSM requires the client workstations to be communicating with the server. If you want to automate your backups for off-hours or weekends, you must enforce a policy that requires users to leave their workstations powered on.

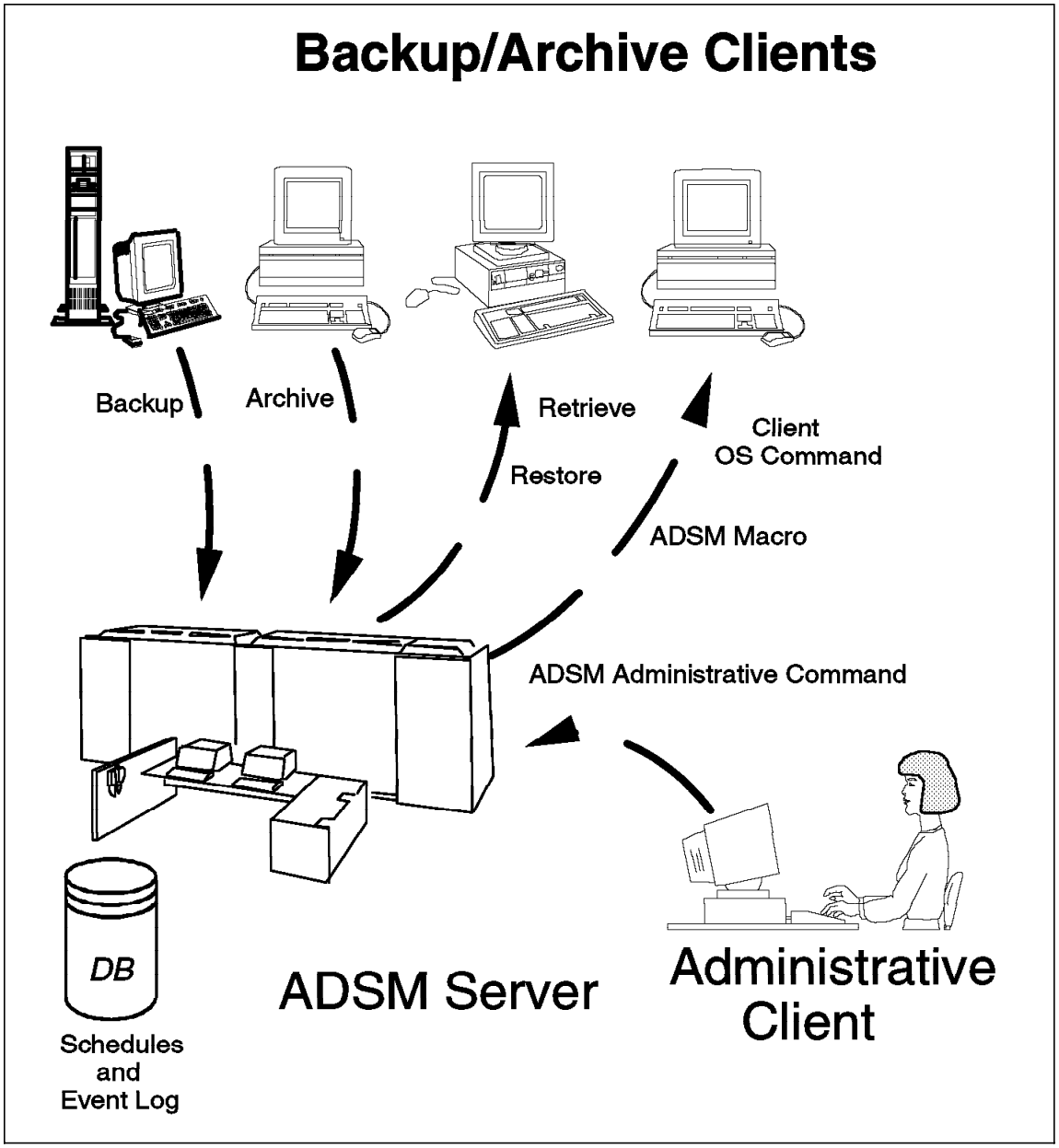


Figure 5. ADSM Central Scheduling

The administrator is responsible for defining and maintaining the schedules and has the authority to prioritize clients so that clients that contain more important data are given preferential treatment.

A schedule event log is maintained in the server database. Whenever a schedule process starts or fails, an event record is written to the log. An administrator can query the log to determine whether scheduled events completed successfully or not.

1.3.4 Policy Management

ADSM enables you to manage the backup and archive process according to policies you establish for your enterprise. The granularity of control that you have is down to the file level. You can decide on how granular you want your policies to be. You can establish an overall system policy, policies by department or organizational structure, or policies by user or file name. Policy management makes ADSM a true system-managed storage implementation. The elements of policy management are discussed below.

1.3.4.1 Policy Domain

A policy domain is a group of clients that are working according to the same set of policy needs. A policy domain provides a logical way of managing backup and archive policies for a group of client nodes. There is no limit to the number of policy domains that can be defined on an ADSM server. Policy domains can be used to provide standard storage management policies to most users, group together clients that have similar storage management requirements, limit the number of clients to be managed by a single policy administrator, and restrict the number of management classes to which users have access.

1.3.4.2 Policy Set

Each policy domain can contain one or more policy sets. A policy set contains one or more management classes. A policy domain can have more than one policy set, but only one policy set can be activated at any one time. Each policy set contains a default management class and can contain any number of additional management classes. Policy domain and policy set information is stored in the server database.

1.3.4.3 Management Class

Policy sets contain one or more management classes. Management classes contain a backup copy group and/or an archive copy group or no copy group.

You can think of management classes as a Service Level Agreement you have with your clients on how their backup and archive data will be handled. There is a concept of binding the management class to the file when it is backed up or archived. Thus the management class is associated with that file. You can rebind a file with a new management class. Users can

use the default management class or explicitly select a management class that is within the active policy set to which they have access.

1.3.4.4 Copy Group

Copy groups are where you specify the parameters that will control the generation and expiration of backup and archive data. There is a copy group for backup and one for archive. In the current ADSM product, all copy groups are named STANDARD. Copy group information is stored in the ADSM server database. Figure 6 on page 14 illustrates some of the ways in which you can control your ADSM file copies. These options are defined for each type of copy; some examples are listed in Figure 6 on page 14. (This figure also shows the HSM Space Management options—these are not really relevant to restores but are listed for completeness.)

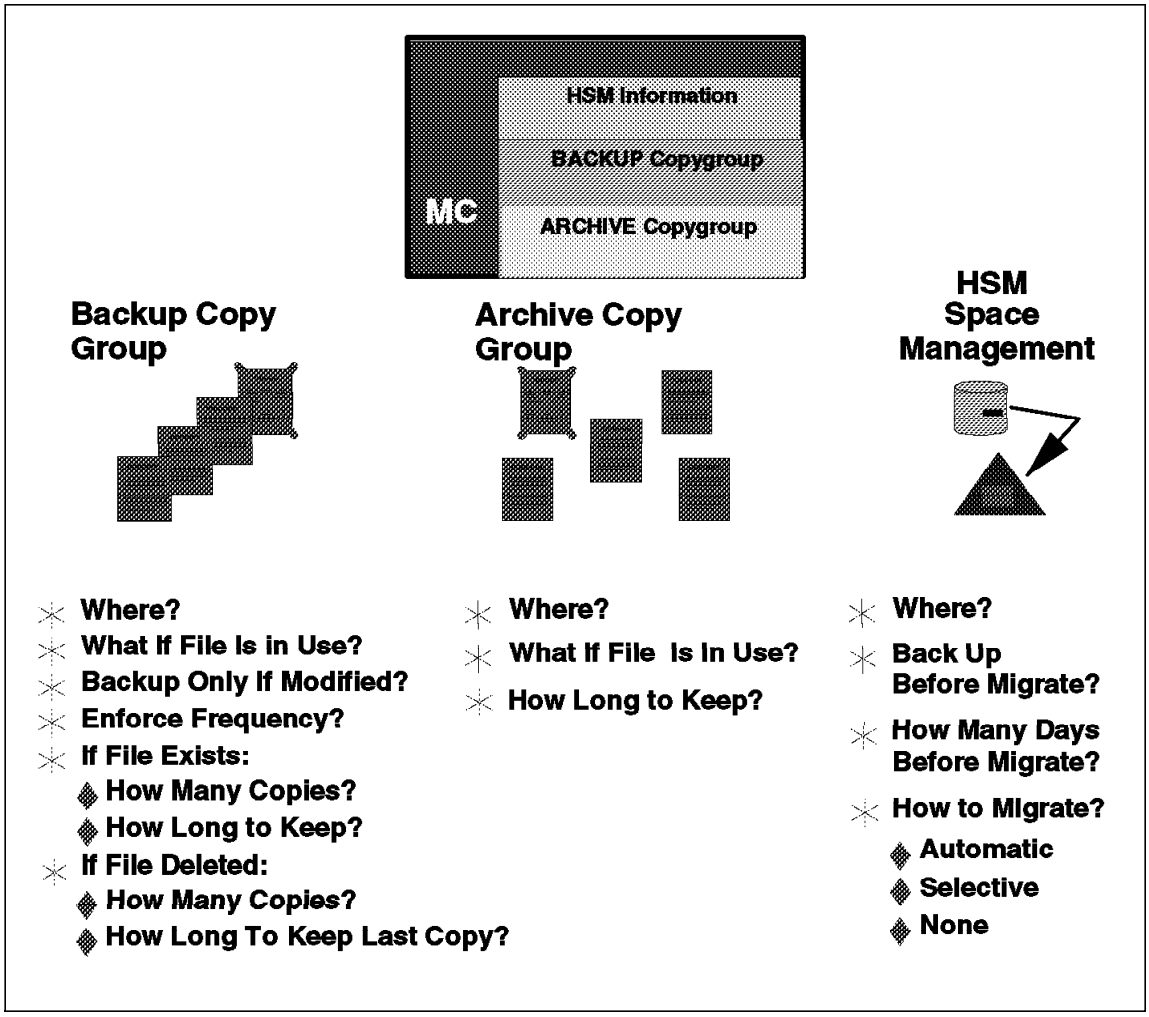


Figure 6. ADSM Copy Group Parameters

Remember that the span of control is at the file level.

Destination specifies the name of the storage pool where the server stores the backed up or archived files.

Frequency for a backup file specifies the minimum number of days that must elapse between incremental backups. This parameter is not used for selective backups. Frequency for an archive file is always command (CMD). A file is archived only when a client issues an archive command or chooses archive from the GUI.

Versioning applies only to backup files. You can specify two different parameters to tell ADSM how many versions of a backup file you want it to maintain. The *Version data exists* parameter specifies the maximum number of different backup versions the server retains for files and directories that currently exist on the client workstation. The most current backup version is called the *active version.* All other versions are called the *inactive versions.*

When the maximum number of versions is exceeded, the server rolls off the oldest version. The *Version data deleted* parameter specifies the maximum number of different backup versions the server retains for files and directories that have been erased from the client workstation.

The *retention period* parameter specifies how long to retain the backed up and archived files. There are two retention parameters for backed up files that correspond to the two types of versioning, and there is one retention parameter for the archived files. *Retain extra versions* specifies how many days the server retains the inactive backup versions when the original file no longer exists on the client's workstation. *Retain only version* specifies how many days the server retains the backup versions it has of a file when the original file has been deleted from the workstation. *Retain version* specifies the number of days an archived copy remains in data storage.

With the *mode* parameter you can specify file backup depending on whether the file has changed since the last backup. This parameter applies to incremental backups, not selective backups. The options for mode are *modified* and *absolute*. *Modified* indicates that you want to back up the file only if it has changed. *Absolute* indicates that you want to back up the file regardless of whether it has changed. For archive files, the mode is always absolute.

Serialization specifies how files or directories are handled if they are modified during the backup or archive process. The serialization parameter has four options: static, shared static, shared dynamic, and dynamic:

- **Static**

  Static specifies that if a file or directory is modified during the backup or archive process, ADSM will not back up or archive the file. The static mode is not supported on the DOS platform.

- **Shared static**

  Shared static specifies that ADSM will retry the backup operation as many times as specified in the client options file. The default is four retries. If the file or directory is modified during each backup or archive attempt, ADSM will not back up or archive the file.

- **Shared dynamic**

Shared dynamic specifies that if a file is modified during a backup or archive attempt, ADSM will backup or archive the file only on its last retry.

- **Dynamic**

  Dynamic specifies that even if the file is modified during the backup or archive attempt, ADSM will back up or archive the file anyway. No retries are required.

1.3.5 Disaster Recovery and ADSM

The critical elements for correct functioning of ADSM are:

- ADSM database

  The database manages information about the location of client backup, archive, and migrated files residing in storage pools, and it records information for ongoing server operations. The database also records storage volume locations for backed up, archived, and migrated files.

- Recovery log

  The recovery log is used to maintain a consistent database image by recording changes made to the database as a transaction proceeds. A transaction is any exchange between a client and the server. If a transaction completes successfully, database changes are committed, and permanent changes are made to the database. If a transaction fails, database changes are undone by removing them from the database and recovery log.

- Storage pools

  The storage pools contain the actual backup, archive, or migrated copies of client files.

1.3.5.1 Database, Recovery Log, and Storage Pool Relationships

Information stored in the ADSM database, recovery log, and storage pool volumes is closely related. The database and recovery log contain cross references to client transactions. As a result of transactions, information, files, or instructions are sent to the storage pool volumes. It is therefore very important that this data be consistent.

If the ADSM database, recovery log, or storage pool volumes is corrupted, the ADSM server becomes unavailable. To assist in the protection and recovery of data, use the following ADSM features:

- Mirror the recovery log and ADSM database

  One of the most catastrophic failures in ADSM is loss of the database or recovery log. To protect against such loss, ADSM provides the capability

to mirror the database and recovery log, which causes the data to be written to multiple disks simultaneously. However, mirroring does not protect against hardware failures that affect multiple drives or against the loss of the entire system (so you should also back up the ADSM database as described below). Administrator control of mirroring can be performed dynamically while ADSM is running.

- Back up the server database periodically on removable media and store the media offsite

  You can take advantage of the capability to make full or incremental backups of the database while ADSM is operational and available to clients. If a disaster occurs, you can use backed up copies to restore the database.

  ADSM provides the capability to recover the database to its most current state (using roll-forward recovery) or to a specific point in time.

- Back up the storage pools periodically on removable media and store the media offsite

  To ensure that a client's file system can always be restored, regularly make backup copies of the primary storage pools (backup, archive, and space management). The backup copies are stored in copy storage pools, which can be used to restore the original files if they become damaged or lost.

  A typical storage hierarchy migrates from disk to tape, with the primary storage pools being on disk. These primary storage pools should be backed up incrementally to the same copy storage pools each day. Backing up to the same copy storage pool ensures that files are not recopied as they migrate to the next storage pool in the hierarchy.

  With correctly scheduled storage pool backups and migrations and with sufficient disk space, most copies can be made from the disk storage pool before the data is migrated to tape, thus avoiding unnecessary tape mounts.

  Backing up storage pools requires additional space requirements in the database. ADSM keeps track of the location, name, and characteristics of all files using the server database. In addition, a small amount of space is needed for internal database indexing. As more files are added, copy storage pools and database storage requirements must be continuously evaluated.

  The best protection against any kind of failure is to mirror the database and recovery log and periodically back up the database and storage pools to offsite media. We also recommend creating volume history and device configuration files.

1.3.6 Disaster Recovery Manager

DRM is available for ADSM Version 2 servers on the AIX and MVS platforms. It performs three main tasks:

- Automatic generation of a server disaster recovery plan
- Offsite disaster recovery media management
- Storage of client machine recovery information

1.3.6.1 Storage of ADSM Client Machine Recovery Information

You can use DRM to store the following ADSM client information:

- Identity and priority of ADSM clients, according to application or business needs
- ADSM client machine information
  - Business priority and machine location
  - Association of one or more ADSM node definitions with a machine
  - Machine characteristics (such as machine type, RAM, hard drives, and network adapters)
  - Recovery instructions
- Boot media requirements
- Associations with recovery media

Once this information about the ADSM client is defined and stored at the ADSM server, it becomes part of the disaster recovery plan and hence is available to assist in the bare metal restore of ADSM clients. For example, in a disaster recovery situation, once the ADSM server has been restored, the following queries could be made to obtain information about how to recover the ADSM client hardware platform. These steps are prior to the use of the ADSM client code for data resoration.

Note: These examples are taken from Chapter 1 of *Disaster Recovery Manager Administrator's Guide and Reference,* GC35-0238, for ADSM on MVS.

When the ADSM administrator issues the following command:

```
QUERY MACHINE BUILDING=20.21 FORMAT=DETAILED
```

ADSM displays a list of client machines in building 20.21 and indicates their restore priority:

```
            Machine Name: DILPER.RZ.UNI-KARLSRUHE.DE
         Machine Priority: 1
                 Building: 20.21
                    Floor: 2
                     Room: 206
             ADSM Server?: No
              Description: Rocky's Server
                Node Name: DILPER
      Recovery Media Name: DASBOOT
         Characteristics?: Yes
   Recovery Instructions?: Yes
```

To determine the location of the boot media for a particular machine, the ADSM administrator would issue the following command:

```
QUERY RECOVERYMEDIA DASBOOT
```

ADSM displays the following information in response:

```
Recovery Media Name  Volume Names  Location  Machine Name
-------------------  ------------  --------  ------------
DASBOOT              VOL1 VOL2     KERKER    DILPER.RZ.UNI-KARLSRUHE.DE
```

To determine the machine-specific recovery instructions for the machine, the ADSM administrator issues this command:

```
QUERY MACHINE DILPER.RZ.UNI-KARLSRUHE.DE FORMAT=RECOVERYINSTRUCTIONS
```

ADSM displays the following information in response:

```
  Recovery Instructions for DILPER.RZ.UNI-KARLSRUHE.DE.
  Primary Contact: Alpir S. Bacher (home: ++49-721-608-4040)
  etc...
```

To determine the hardware requirements for machine DILPER.RZ.UNI-KARLSRUHE.DE, the ADSM administrator issues this command:

```
QUERY MACHINE DILPER.RZ.UNI-KARLSRUHE.DE FORMAT=CHARACTERISTICS
```

ADSM displays the following information in response:

```
Intel Pentium 160MHz,64MBytes RAM,SCSI adapter 1GByte hard drive
SCSI CDROM, 3COM EtherlinkIII network adapter
Partitioning of Hard Drives:
BootManager
C: DRIVE_C logical partition 200 MBytes
D: DRIVE_D logical partition 450 MBytes
E: DRIVE_E logical partition 200 MBytes
F: DRIVE_F logical partition 150 MBytes
etc...
```

1.3.6.2 ADSM Client Bare Metal Restore

The ability of DRM to store ADSM client machine and recovery information at the ADSM server is most pertinent to us in the context of bare metal restore of ADSM clients.

The recovery of ADSM clients presupposes the existence of a recovery plan to re-create the hardware, operating system, and communications environment necessary to run the ADSM client code before that client's file systems can be restored from the ADSM server storage pool.

Although the DRM feature currently does not contain automation to aid in the recovery of the underlying ADSM client hardware, operating system, and communications software, it does permit the storage of such instructions at the ADSM server as client recovery information. Hence, in a disaster recovery situation, after you have used DRM to restore the ADSM server, you can also use it to retrieve information about how to undertake the bare metal restore of the ADSM clients.

Of course, the DRM feature is not a prerequisite to using the bare metal restore techniques we describe in this book. Information about the steps necessary to restore the ADSM client platform in the stages before using the ADSM client code (namely, restoring the hardware, partitioning hard drives, restoring the operating system software, communications, and ADSM client code), although conveniently stored at the ADSM server by using DRM, can also be stored elsewhere (for example, on hardcopy stored offsite, or in a file on another machine).

Chapter 2. OS/2 Warp V3: Bootable, Direct Recovery

In this chapter we explain how to use bootable diskettes to recover a single OS/2 Warp V3 desktop client environment that uses TCP/IP or NetBIOS to communicate with its ADSM server. We review the kind of information to back up in preparation for a disaster, explain how to create bootable diskettes, and discuss how to use the bootable diskettes in conjunction with the saved information to recover after a disaster.

It is also possible to use configuration, installation, and distribution (CID) peer recovery for this platform. Refer to Chapter 6, “Recovery of OS/2 and Windows from an OS/2 CID Peer” on page 107 for information about using CID peer recovery for clients that use Advanced Program-to-Program Communication (APPC) ADSM communications.

2.1 Product Overview

OS/2 WARP Version 3 is an advanced 32-bit operating system. It provides functions such as multitasking and multithreading. It runs 32-bit applications as well as 16-bit DOS and Windows programs. It also provides variety of networking services such as Internet, office, and remote access.

OS/2 provides two different kinds of file systems: the file allocation table (FAT) file system and the high-performance file system (HPFS). The FAT system is similar to the DOS FAT system. File names are restricted to eight characters with a three-character delimiter. HPFS uses high-speed buffer storage known as cache to provide fast access to large disk volumes. It also supports the coexistence of multiple, active file systems on a single desktop, using multiple, different storage devices. HPFS file names can be as many as 254 characters long.

OS/2 Warp Version 3 is a single-user environment, so security tends to be handled with such mechanisms as lock words.

2.2 Predisaster Preparation

The disaster we are preparing for is the total and catastrophic loss of the ADSM client, where provision has to be made to restore everything from the bare metal up. If our disaster recovery preparations can cover this worst case scenario, we can assume that they will also be able to handle recovery from lesser disasters.

In this section we discuss the information to collect and save before a disaster to enable a bare metal restore.

2.2.1 ADSM Backups

If recovery of the operating system is to be from ADSM, a full backup must be taken that includes system files. This is not the default. These system files will of course be specific to the configuration of the machine being backed up. Figure 7 shows the predisaster normal backups being taken.

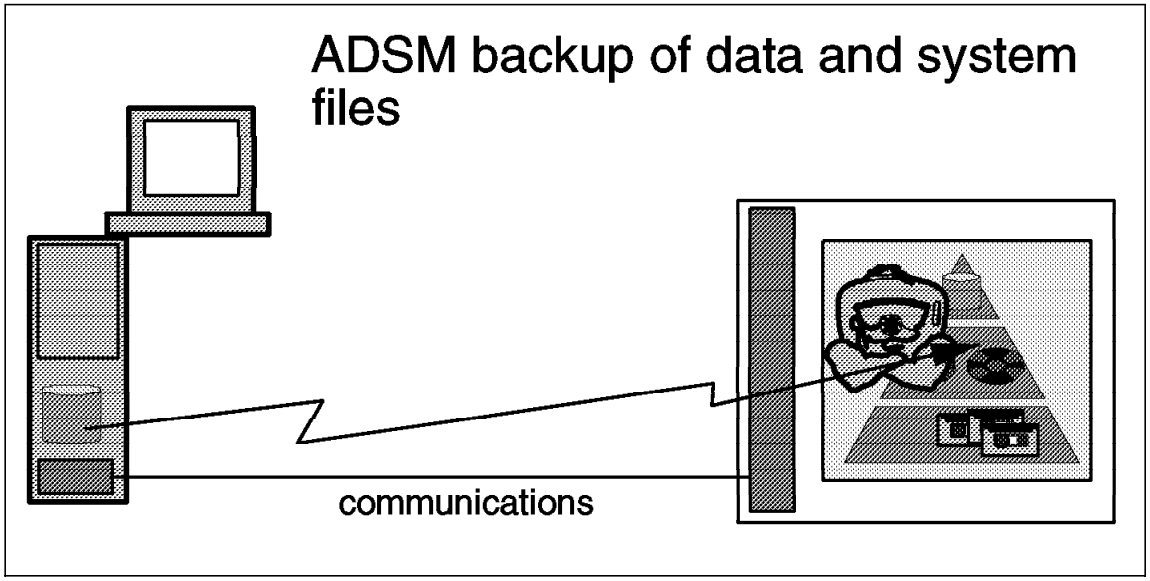


Figure 7. Full ADSM Backup of OS/2 Warp V3 System and Data Files

We recommend that you use the following options for the ADSM backup that you will use for the bare metal restore:

- Set the **Copy Serialization** parameter in the **Backup Copy Group** definition to **Shared Static** This setting allows only those files not being modified to be included in the ADSM backup (preventing a ″fuzzy″ backup). When using this setting, it is best to schedule the ADSM backup during a period of low utilization of the ADSM client. Because this ADSM backup is oriented to provide an image of the workstation to be used in case of disaster, all applications and subsystems running on the machine should be closed before the backup, so that you have the fewest number of open files.
- Because we depend on the existence of an ADSM backup that would provide full restoration of the ADSM client being recovered, we recommend that the ADSM options file, **DSM.OPT**, only EXCLUDE the SWAPPER.DAT and the EA DATA.SF files. This recommendation implies that you include the operating system software on the C: drive in the ADSM backup. The bootable diskettes will provide only a skeleton version of OS/2 that will enable the ADSM client to function. The

assumption is that the newly booted system with the ADSM client will be used to restore the rest of the OS/2 system from an ADSM backup done *for that client.* This may be contrary to your current backup policy (you may currently deliberately EXCLUDE the C: drive from your ADSM backups). This backup should also include empty directories.

2.2.2 Operating Environment of the ADSM Client

In preparation for disaster recovery, we recommend that you collect and save offsite the information listed below in addition to the ADSM backup data. Depending on your installation, you could save this information by using the DRM feature, or you could save it on hardcopy stored offsite. The way in which you save the information is not as important as ensuring that it is saved **somewhere** where it can be easily retrieved along with the client recovery media when a disaster occurs.

- **Hardware configuration**

  Keep information about machine type, bus type, hard disk attachment, and of course, the type of network adapter used. Collect any such information that will help you re-create the hardware setup of the ADSM client that has been destroyed in a disaster. If you are using a PS/2, for instance, you may also include information about where to find copies of the associated PS/2 hardware reference diskettes in case you find yourself needing to replace a hard disk.

- **Partitioning drives**

  Record how the hard drives are partitioned and labeled. You can collect this information by using the FDISK command. To do the restore, ADSM has to know the hard drive label. We recommend that you define hard drive labels that include the drive letter, to make it easier to determine which ADSM filespace should be restored to which drive at disaster recovery time.

- **Communication details**

  Specific information about your installation communications setup (for example, TCP/IP addresses of the ADSM client and server; SUBNET, ROUTE, and DOMAIN name; and TCP/IP port number of the ADSM service and ADSM node name). This information could be customized on the bootable diskettes. However, if one set of bootable diskettes will be used to service many OS/2 clients, you may want to store this data for each individual client (using offsite hardcopy or DRM).

Optional: Statistics for Postdisaster Recovery Verification

You may want to gather and save information that can be used after a disaster recovery test once the restore process is completed, to validate that all information has indeed been restored correctly. Each installation will have its own ideas about the best way to verify that the recovery is complete. Some possible sources of information for recovery verification are:

- ADSM statistics at the end of the backup, such as the Number of Objects Inspected, would give a tally of the directories and files on the client being backed up.
- CHKDSK command output for each backed up disk

  Run CHKDSK for each drive being backed up and record:

  – *X* number of kilobytes used in *A* number of directories

  – *Y* number of kilobytes used in *B* number of user files

  – *Z* number of kilobytes used in extended attributes

  For FAT drive records:

  – *X* number of kilobytes used in *A* hidden files

  – *Y* number of kilobytes used in *B* number of directories

  – *Z* number of kilobytes used in *C* user files
- DIR command output

  Collect the output of the DIR /A /S command in a file for each drive. After disaster recovery testing, use the output to compare the files available before the test. Utilities such as the AIX DIFF program could be used for this kind of comparison.
- Other test scripts used during your installation's periodic disaster recovery tests.

2.2.3 Creating the Bootable Diskettes

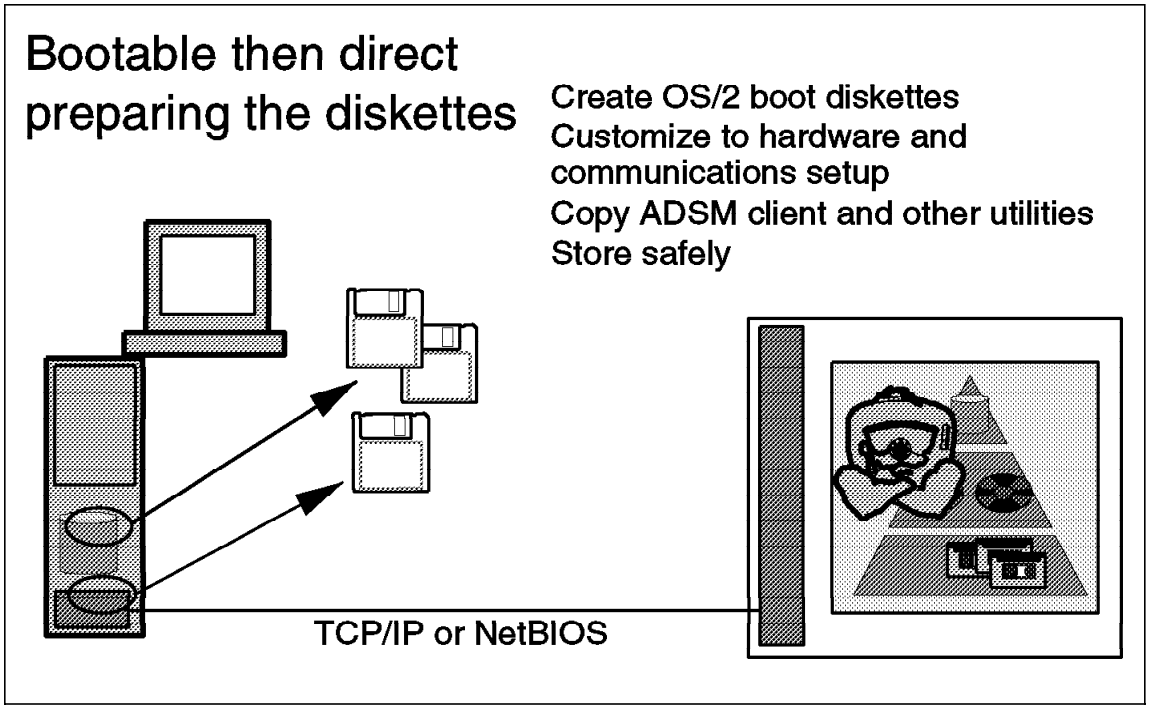


Figure 8. Creating the Bootable Diskettes: OS/2 Warp V3

In this section we describe a technique for creating bootable diskettes for OS/2 Warp. After a disaster, you use these diskettes to quickly boot a replacement machine with the minimal operating system, communications, and ADSM software necessary to begin file restoration with the ADSM client and server. Normal ADSM recovery can then be used to recover the remainder of the predisaster client environment.

2.2.3.1 Assumptions

Our instructions for creating bootable diskettes apply to OS/2 machines using TCP/IP or NetBIOS through a token-ring adapter. We tested only the TCP/IP method but include the NetBIOS instructions as well for your reference. *Modifications may be necessary for this technique to work in environments using other network adapters, hard disk controllers, and so on.*

These instructions apply to the following products:

- OS/2 Version 2.x
- OS/2 Version 3.0 (Warp)
- OS/2 Version 3.0 (Warp Connect)
- IBM TCP/IP V2.0

- IBM TCP/IP V3.0
- ADSM/2 Version 1, Release 2 client code
- ADSM/2 Version 2, Release 1 client code
- Any ADSM server that uses TCP/IP or NetBIOS

A complete ADSM backup as described in 2.2, “Predisaster Preparation” on page 21 should be available at the ADSM server, and the restore should be done to a hardware configuration similar to that of the original ADSM backup/archive client machine.

2.2.3.2 Configuration Used to Test the Technique

We tested the technique on two hardware configurations:

An ADSM client with:

- PS/2 Model 95 with 32 MB of RAM
- 16 Mbps token-ring attachment
- SCSI-attached hard disks
  - C: 160 MB
  - D: 160 MB
  - E: 320 MB
- OS/2 Warp Version 3.0
- TCP/IP Version 2.0
- HPFS
- ADSM/2 Version 2, Release 1, Level 0.3 client code
- ADSM/AIX Version 2, Release 1, Level 0.2 server code

An ADSM client with:

- Personal Computer 750 with 32 MB of RAM
- 16 Mbps token-ring attachment
- ISA/PCI attached hard disks
  - C: 1.6 GB
- OS/2 Warp Version 3.0
- TCP/IP Version 3.0
- HPFS
- ADSM/2 Version 2, Release 1, Level 0.3 client code

– ADSM/AIX Version 2, Release 1, Level 0.2 server code

To use this technique you will need:

- Three blank formatted 1.44 MB diskettes
- OS/2 system installation diskettes (depending on the technique selected for creating the bootable diskettes)
- If you are using PS/2 hardware, the associated hardware reference diskettes may be useful.

2.2.3.3 Step-by-Step Instructions

These instructions for creating a set of OS/2, TCP/IP or NetBIOS, ADSM/2 client enabled bootable diskettes are based on the method provided by Kenneth Morse of the IBM Washington Systems Center.

Step 1: Create the Base OS/2 Diskettes: Booting an OS/2 system requires two diskettes. The first is identical to your installation disk 0 (and is henceforth referred to as disk 0). The second is similar to your installation disk 1, as it contains the command line OS/2 (CMD.EXE), your CONFIG.SYS file, and any drivers that are loaded at boot time.

There are many ways in which you can create these diskettes. We created the base diskettes by copying the original installation diskettes (works for OS/2 2.x and OS/2 Warp only). For alternative methods, refer to Appendix A, “Alternative Methods to Create Base OS/2 Bootable Diskettes” on page 269.

To create the base diskettes, use DISKCOPY to make copies of the original OS/2 installation disks 0 and 1. This is not simple, as the original diskettes are configured to install OS/2, not drop directly to CMD.EXE. They also contain some installation files, which you have to carefully remove to make room for TCP/IP on the diskettes.

Step 2: Edit Base OS/2 Diskettes by Deleting Files: Remove the following files from disk 1:

- **OS/2 Version 2.x**

  ```
  BUNDLE.
  FDISK.COM
  SYSINST2.EXE
  MOUSE.SYS
  ```

- **OS/2 Warp**

```
OS2LOGO.
BUNDLE.
FDISK.COM
SYSINST2.EXE
XDFLOPPY.FLT
DEL.LST
MOUSE.SYS
```

- **OS/2 Warp Connect**

  Do not try to use this technique to create bootable diskettes from OS/2 Warp Connect diskettes. It is not practical because of the way they are packaged. Use the CID creation method described in Appendix A, "Alternative Methods to Create Base OS/2 Bootable Diskettes" on page 269 instead.

Step 3: Edit the Base OS/2 Diskettes to Add Files: Once you create the base OS/2 diskettes, add the following files:

- **OS/2 files**

  Below is a list of OS/2 files that you must copy to or create and then copy to disk 1.

```
File Name     Found in
---------------------------------------
VDISK.SYS   - \OS2 -or - \OS2\BOOT
NLS.DLL     - \OS2\DLL
STARTUP.CMD - See B.1, "STARTUP.CMD" on page 271.
FINDRAM.CMD - See B.2, "FINDRAM.CMD" on page 271.
THE.CMD     - See B.3, "THE.CMD" on page 272.
PART2.CMD   - See B.4, "PART2.CMD" on page 273.
PART3.CMD   - See B.5, "PART3.CMD" on page 274.
SETUP.CMD   - See B.7, "SETUP.CMD" on page 276.
An editor   - To dynamically choose your settings at
              boot time, you must have a copy of a tiny
              editor (for example, TEDIT, which comes with
              OS/2 Warp).  Any editor will do, as long as it
              does not need a graphical interface and fits
              on the 1.44 MB diskette.
```

- **LAN support files**

  You must have the support layer necessary to operate your network card at the hardware level. Below is a list of files that you have to add to disk 1. Next to each file name is a hint as to where to find it on a working LAN-attached system.

```
File Name     Found in
---------------------------------------
LANMSGEX.EXE - \IBMCOM
PROTOCOL.INI - \IBMCOM
LANMSGDD.OS2 - \IBMCOM
PROTMAN.OS2  - \IBMCOM
LT0.MSG      - \IBMCOM
LT2.MSG      - \IBMCOM
PRO.MSG      - \IBMCOM
LANMSGDL.DLL - \IBMCOM\DLL
IBMTOK.OS2   - \IBMCOM\MACS
NETBIND.EXE  - \IBMCOM\PROTOCOL
```

Depending on your setup, you may have to replace IBMTOK.OS2 with whatever NDIS driver is appropriate for your network adapter. IBMTOK.OS2 works well for most variations of IBM token-ring adapters. For other adapters, you have to determine which NDIS driver you are using. If you do not know which driver you are using, try looking in the following places:

- In PROTOCOL.INI, all of your protocols should be bound to one driver. The internal name of the driver, for example, IBMTOK$, should be awfully close to the file name, for example, IBMTOK.OS2.
- Load up Multi-Protocol Transport Support (MPTS) and look at the driver that is loaded. Many of the driver descriptions list the file name of the driver in parentheses next to the driver's name.
- Look through CONFIG.SYS. Some drivers, such as IBMETHRN.OS2, jump right out at you.

- **TCP/IP Version 2.0 files**

  For TCP/IP Version 2.0 support, the following files must be copied from a working TCP/IP Version 2.0 system to disk 1:

```
File Name     Found in
---------------------------------------
CNTRL.EXE    - \TCPIP\BIN
IFNDIS.SYS   - \IBMCOM\PROTOCOL
INET.SYS     - \IBMCOM\PROTOCOL
```

- **TCP/IP Version 3.0 files**

  For TCP/IP Version 3.0 support, the following files need to be copied from a working TCP/IP Version 3.0 system to disk 1:

```
File Name     Found in
---------------------------------------
CNTRL.EXE    - \MPTN\BIN
IFNDIS.SYS   - \MPTN\PROTOCOL
SOCKETS.SYS  - \MPTN\PROTOCOL
AFINET.SYS   - \MPTN\PROTOCOL
```

Attention: TCP/IP Version 3.0/MPTS Version WR82xx

If you are building from a TCP/IP Version 3.0 (Warp Connect) system, we recommend that you use a system with no MPTS maintenance applied. Many of the executables from later versions of MPTS (most notably WR08200) have been built in such a manner that they will not work correctly from diskettes. ARP.EXE, HOST.EXE, IFCONFIG.EXE, PING.EXE, and ROUTE.EXE from WR08200 were all linked to require PMMERGE.DLL, a 1 MB file! As of this writing, the latest level of MPTS is WR08210, at which the only module that requires PMMERGE is PING.EXE.

Your best chance of success is with the MPTN shipped with base Warp Connect. Do **not** try to use WR08200! If you have no choice, upgrade to WR08210 by using CSD service; do not use PING.EXE.

- **NetBIOS files**

  For NetBIOS support, the following files must be copied from a working NetBIOS system to disk 1:

```
File Name      Found in
---------------------------------------
NETBEUI.OS2  - \IBMCOM\PROTOCOL
NETBIOS.OS2  - \IBMCOM\PROTOCOL
```

Step 4: Modify CONFIG.SYS: Make the following modifications to the CONFIG.SYS file on disk 1:

- **Resolve references to previously deleted files**

  In Step 2 we deleted the following files:

```
XDFLOPPY.FLT (OS/2 Warp)
MOUSE.SYS    (OS/2 Version 2.X and OS/2 Warp)
```

  Remove references to these files from CONFIG.SYS.

- **Change path statements**

  Change the three path statements so that they reference the A:drive and the current directory. We recommend that you change them to the following:

```
LIBPATH=.;\;A:\;
SET PATH=.;\;A:\;
SET DPATH=.;\;A:\;
```

- **Set up initialization**

  In order for STARTUP.CMD to be properly executed, it must be referenced by the OS2_SHELL environment variable. Make sure you have a line that looks like this:

  ```
  SET OS2_SHELL=CMD.EXE /K STARTUP.CMD
  ```

  as well as:

  ```
  PROTSHELL=SYSINST1.EXE
  ```

- **Reference device drivers**

  All of the device drivers copied to disk 1 must be referenced. Add the following lines to the bottom of CONFIG.SYS (naturally you would include either the TCP/IP Version 2.0 *or* TCP/IP Version 3.0 stanza, not both):

  ```
  REM *** PROTOCOL/LAN/VDISK DRIVERS ***
  DEVICE=\VDISK.SYS 4069,,
  DEVICE=\LANMSGDD.OS2 /I:A:\
  RUN=\LANMSGEX.EXE
  DEVICE=\PROTMAN.OS2 /I:A:\

  REM *** Appropriate Network Adapter Driver Here ***
  DEVICE=\IBMTOK.OS2

  REM *** TCP/IP VERSION 2.0 DRIVERS ***
  DEVICE=\INET.SYS
  DEVICE=\IFNDIS.SYS
  RUN=\CNTRL.EXE

  REM *** TCP/IP VERSION 3.0 DRIVERS ***
  DEVICE=\SOCKETS.SYS
  DEVICE=\AFINET.SYS
  DEVICE=\IFNDIS.SYS
  RUN=\CNTRL.EXE

  REM *** NETBIOS DRIVERS IF YOU PLAN TO USE THEM ***
  DEVICE=NETBEUI.OS2
  DEVICE=NETBIOS.OS2

  REM *** NETBIND ***
  RUN=\NETBIND.EXE
  ```

- **Edit PROTOCOL.INI**

Copy the PROTOCOL.INI file from the hard drive of a working system to disk 1. To the best of our knowledge, the following stanzas are required:

```
The Protocol Manager          PROT_MAN
The NetBIOS Protocol          NETBIOS
The NetBEUI Protocol          NETBEUI_nif
The TCP/IP Protocol           TCPIP_nif
The appropriate NDIS driver   IBMTOK_nif
```

Chances are all of these stanzas are present in a working system that uses TCP/IP and/or NetBIOS. If one or more of these stanzas is missing, try to find another machine with the missing stanza and steal it (the stanza, not the machine). Keep in mind that:

- The name of the stanza need not match exactly with the name we used above.
- The stanza of each protocol (TCP/IP, NetBIOS, and NetBEUI) should have a statement binding it to the network card′s driver.
- Extra stanzas are OK.
- On the cards that require it, make sure you select the correct network speed.
- If your adapted stanza contains a line specifying your Locally Administered Address, you may want to remove it, so that multiple machines can use the same diskettes without causing a conflict.

Step 5: Create Disk 2: To create disk 2, collect files in a temporary directory, compress them into a zip file, and copy the resulting zip file onto disk 2 with the appropriate decompression utility.

You will need a pair of compression/decompression utilities. We cover the use of PKWare′s PKZIP2/PKUNZIP2 and InfoZip′s ZIP/UNZIP. Disk 2 will contain compressed versions of the ADSM client and TCP/IP (and/or NetBIOS) files, OS/2 utilities, and an appropriate decompression utility. Here are the steps to create disk 2:

- **Create a temporary directory**

  To collect all necessary files, create a new directory called something like C:\TEMPADSM:

  ```
  MKDIR C:\TEMPADSM
  ```

  - ADSM client files

  Copy the following ADSM files from a working ADSM client to the \TEMPADSM directory you have created:

```
DSCAMENG.TXT   - Assuming American English
DSMADMC.EXE    - Only if Administrative Client is required
DSMC.EXE
DSMC.HLP
FCLCNRP.DLL
HPFS386.DLL
NAMPIPES.DLL   - from the \OS2\DLL directory
```

- TCP/IP files

You must copy the following TCP/IP files (from your TCPIP or MPTN subdirectories) into \TEMPADSM in order to use TCP/IP:

```
ARP.EXE
IFCONFIG.EXE
PING.EXE
ROUTE.EXE
TCPIPDLL.DLL    - From the \TCPIP\DLL or \MPTN\DLL directory
PROTOCOL.       - Yes, the file Protocol. has no extension
                  From the \TCPIP\ETC or \MPTN\ETC directory
```

- NetBIOS files

Copy the following file into \TEMPADSM if you are going to use NetBIOS:

```
Filename      Found in
------------------------
ACSNETB.DLL   \IBMCOM\DLL
```

- OS/2 utilities

The following utilities are not required to successfuly run ADSM, but they can come in quite handy, so copy them to \TEMPADSM:

```
FDISK.COM    - For repartitioning
FORMAT.COM   - For reformatting
LABEL.COM    - For changing volume names
CHKDSK.COM   - For repairing file system damage
UHPFS.DLL    - Required for HPFS partition work
ATTRIB.EXE   - For altering file attributes
MAKEINI.EXE  - For repairing or rebuilding .INI files
XCOPY.EXE    - For copying files
INI.RC       - Seed file for MAKEINI
INISYS.RC    - Seed file for MAKEINI
LOCK.RC      - Seed file for MAKEINI
NETSTAT.EXE  - For checking the network
SYSINSTX.COM - For bootstrap sector initialization
OSO001.MSG   - OS/2 message repository. Due to space
               restrictions don't put this file on Disk 1.
               This is the stock OS/2 message file.  When you
               finally use these diskettes to boot OS/2, you will
```

```
get a SYS0318 message stating that the operating
system could not find message 1467.
If you were to type
HELP SYS1467 on a different machine, you would see

SYS1467: VDISK Version 2.1 Virtual Disk ***
Disk Size:          *** KB
Sector Size:        ***
Directory Entries:  ***

In other words, don't worry about it!
```

Feel free to include any other small utilities you think may come in handy when working on a damaged system; your only limit is the amount of data that can be compressed to fit on a 1.44 MB diskette.

- **Build the zip file**

  If you use the PkZip2 and PKUnZip2 utilities with C:\TEMPADSM as the temporary directory, execute the following commands to build the zip file on disk 2:

  ```
  C:
  CD C:\TEMPADSM
  PKZIP2 ADSMPACK.ZIP *
  ```

  If you are using the ZIP and UNZIP utilities, execute the following commands to compress all of the files you gathered together into a file named ADSMPACK.ZIP:

  ```
  C:
  CD C:\TEMPADSM
  ZIP ADSMPACK.ZIP *
  ```

  Copy this file to disk 2.

- **Copy the decompression utility**

  Copy the corresponding decompression program (PKUNZIP2.EXE or UNZIP.EXE) to disk 2. If you use InfoZip's UNZIP.EXE, you will have to copy the NLS.DLL file from your \OS2\DLL subdirectory onto disk 2.

Make sure you edit PART2.CMD on disk 1 and specify which decompression utility you will be using!

2.3 Postdisaster Recovery

In this section we describe how to recover from a disaster to the OS/2 ADSM client by using the information you saved before the disaster (described in 2.2, "Predisaster Preparation" on page 21), the subsequent

ADSM backup data, and the bootable diskettes you created (described in 2.2.3, “Creating the Bootable Diskettes” on page 24.)

To simulate a disaster, we physically swapped the C: and D: drives of the PS/2 Model 95 so that OS/2 would no longer boot.

To recover, we rebuilt the hardware environment, booted the recovery system, and restored from the ADSM backup.

2.3.1 Rebuild Hardware Environment

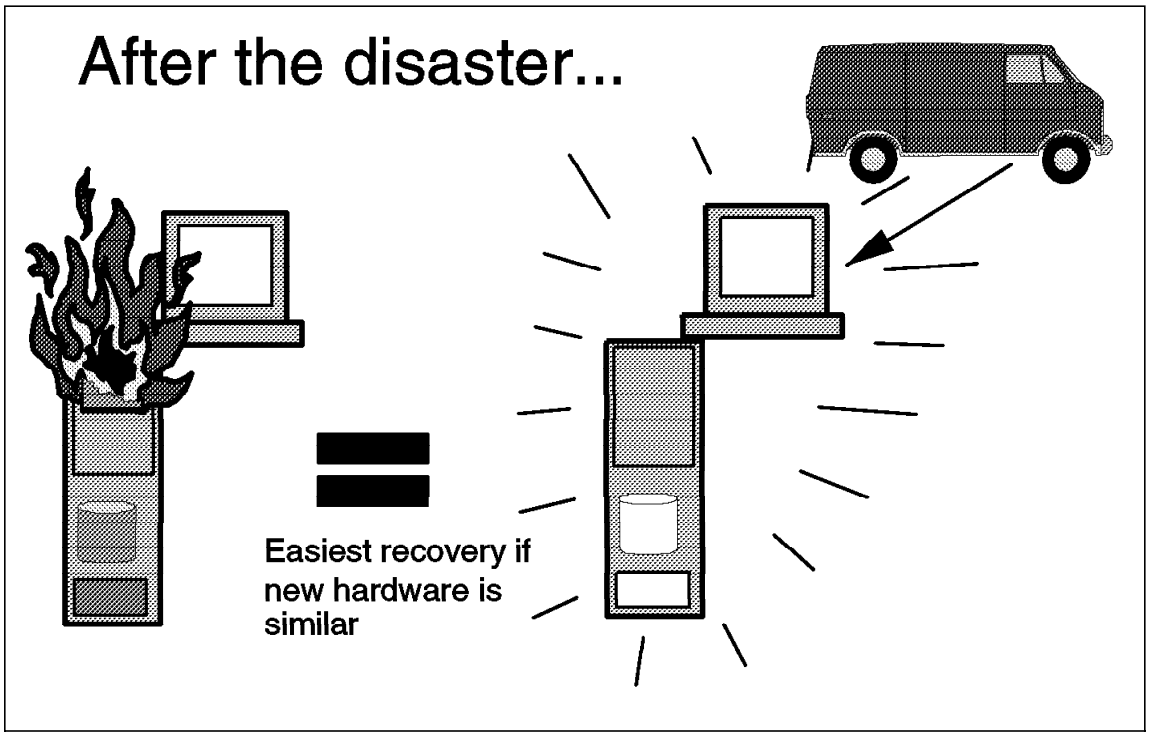


Figure 9. Obtain Suitable Replacement Hardware: OS/2 Warp V3

Retrieve information about the OS/2 machine to help re-create the hardware environment of the destroyed ADSM client. The new replacement machine must have a similar configuration.

If DRM had been used as the repository for this type of information, you can retrieve it by issuing the appropriate ADSM queries to the ADSM server. For examples of these queries, see 1.3.6, “Disaster Recovery Manager” on page 18.

2.3.2 Boot the Recovery System

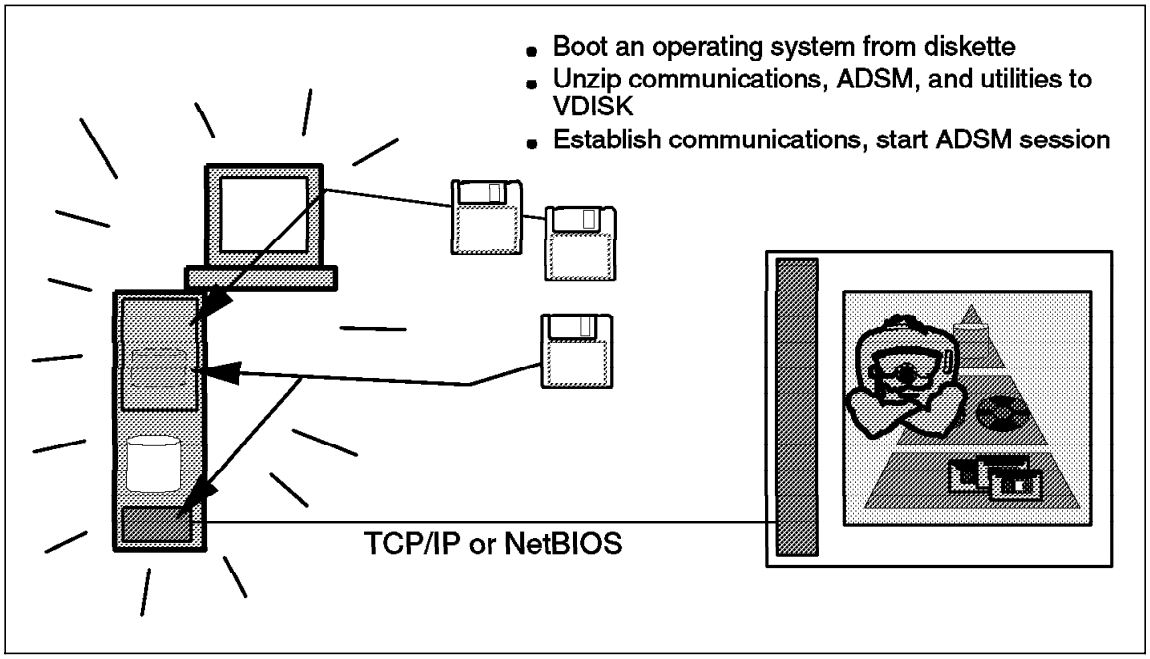


Figure 10. Boot OS/2 Warp V3 Recovery System

Use the OS/2 Warp Version 3 bootable diskettes to boot the replacement hardware and prepare for ADSM file recovery. Follow these steps:

1. Boot the machine with disk 0, until the blue screen asking for disk 1 appears.
2. Insert disk 1 and press <ENTER>. Wait for the message asking for disk 2. At this point you see on the screen:

```
ADSM BOOTABLE RECOVERY STARTED.........
*********************************************

Searching for a VDISK
VDISK Found as drive (E:\)

Copying files to drive (E:\)

Unpacking file to VDISK
Wait for all diskette activity to stop, (background processes..)
Remove diskette 1 from the drive, and insert diskette 2 and then
Press any key when ready  . . .
```

3. Wait for all activity to stop, remove disk 1, insert disk 2, and press <ENTER>. Wait for the message requesting disk 1 again:

```
Working...
PKUNZIP (R) FAST!  Extract Utility  Ver. 1.09-OS/2 Prot Mode 1-15-91
Copr. 1989-1991 PKWARE Inc. All Rigths Reserved PKUNZIP/h for help
PKUNZIP Reg. U>S> Pat. an Tm. Off.     IBM LICENSED VERSION


Searching ZIP: A:ADSMPACK.ZIP
  Exploding: UHPFS.DLL
  Exploding: XCOPY.EXE
  .
  .
  .
  Exploding: UHPFS.DLL
  Exploding: XCOPY.EXE
Done...
Please remove diskette 2 from the drive, and insert diskette 1 and then
Press any key when ready  . . .
```

4. After you remove disk 2, insert disk 1, and press <ENTER>. The tiny editor TEDIT.EXE shows the contents of SETUP.CMD, which contains ADSM configuration setup information. Normally there is no reason to edit SETUP.CMD unless you are using one set of OS/2 bootable diskettes for several clients and must tailor it to reflect individual machine characteristics. If you have to make changes to SETUP.CMD you can save the changes by pressing F4.

5. After the Initialization Complete message appears, the OS/2 prompt appears. At this point you can start the ADSM restore.

```


Configuring ADSM

Configuring ADSM TCP/IP

Configuring TCPIP

Starting TCP/IP

Initialization Complete:  You may now start the ADSM restore...

E:\
```

2.3.3 Restore from the ADSM Backup

We outline some recovery scenarios below.

2.3.3.1 Restoring the Whole System

Now that you have booted the desktop with your OS/2 bootable diskettes, you can invoke the ADSM command line client and take the following steps to restore the entire system as shown in Figure 11:

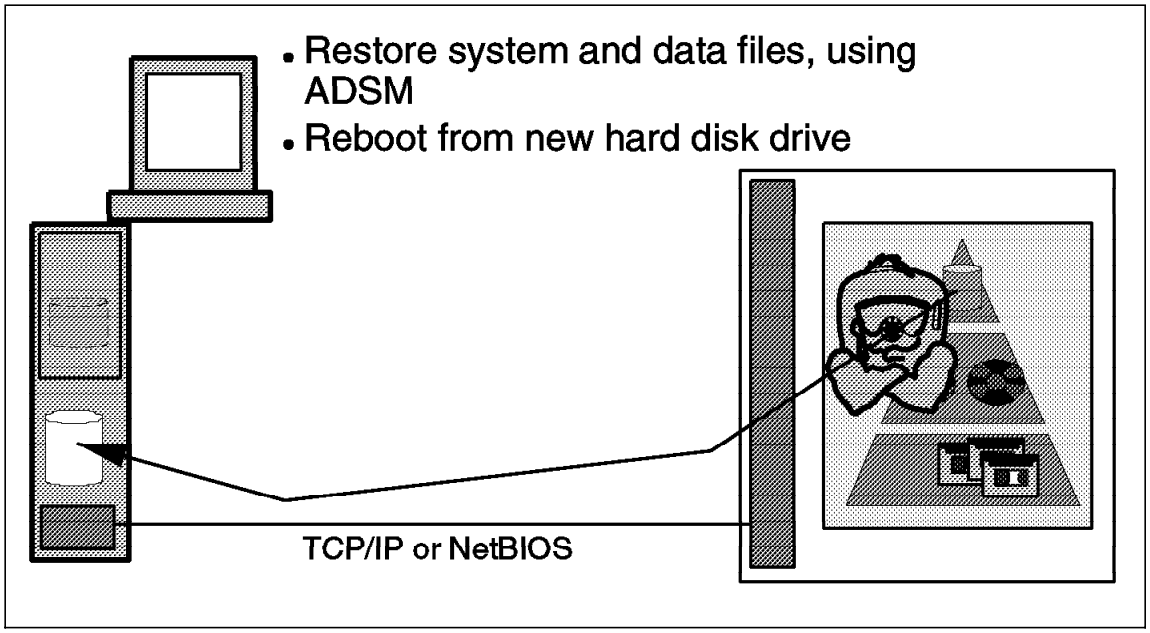


Figure 11. Use the ADSM Command Line Client to Recover the OS/2 Disk(s)

1. ADSM identifies hard drives by their volume name, so you have to ensure that the new hard drive has the same setup as the original. Use DRM to obtain this information, or query ADSM to find out how you should label the drives:

   ```
   DSMC QUERY FILESPACE
   ```

Volume Name Considerations

Note that a QUERY FILESPACE will tell you which volume labels ADSM expects to see. It does not tell you which drive letters should be assigned to them. It your drives are not labeled in a self-describing fashion, information about how they are partitioned must be saved before a disaster. For example, ADSM tells us that a system is laid out as follows:

```
Num     Last Incr Date      Type    File Space Name
---     --------------      ----    ---------------
  1   08/26/1996 04:20:46               HPFS     DRIVE-D
  2   08/26/1996 04:20:13               FAT      DRIVE-C
```

This poses no problem; we format drive C: as FAT and name it DRIVE-C and format drive D: as HPFS and name it DRIVE-D. If ADSM returns the following, however:

```
Num     Last Incr Date      Type    File Space Name
---     --------------      ----    ---------------
  1   08/26/1996 04:21:22               HPFS     RAUL
  2   08/25/1996 04:20:00               FAT      DOS63
  3   08/26/1996 04:20:13               HPFS     OS221
  4   08/26/1996 04:20:46               FAT      CARMEN
  5   08/26/1996 04:25:72               LAN      ALEJANDRA
```

you must store the information like this before the disaster (perhaps using DRM at the ADSM server):

```
Drive C: - FAT   - DOS63      \ Two primary partitions under
Drive C: - HPFS  - OS221      / the control of boot manager
Drive D: - FAT   - CARMEN     - Data drive
Drive E: - HPFS  - RAUL       - Data drive
Drive F: - LAN   - ALEJANDRA  - LAN home directory
```

2. Partition the hard drive, using FDISK, and reboot.
3. Format the partitions, for example:

```
FORMAT C: /FS:FAT
FORMAT D: /FS:HPFS
```

4. Restore all files from ADSM:

```
DSMC RESTORE C:\* -SUBDIR=YES -REPLACE=YES
DSMC RESTORE D:\* -SUBDIR=YES -REPLACE=YES
```

5. Reboot the system from the hard drive.

Still assuming that you are working from your OS/2 bootable diskettes, here are some other restoration scenarios:

2.3.3.2 Restoring the OS/2 Desktop

To replace all objects on your OS/2 desktop, assuming that it was saved during a recent ADSM incremental backup, you can get it back by doing the following:

1. Remove the ruined desktop:

   ```
   MOVE C:\DESKTOP \OLDDESK
   ```

2. Restore your saved desktop, using this ADSM command:

   ```
   DSMC RESTORE C:\DESKTOP\* -SUBDIR=YES
   ```

3. Restore your desktop program information, with this ADSM command:

   ```
   DSMC RESTORE C:\OS2\OS2*.INI -REPLACE=ALL
   ```

4. Reboot your system from the hard disk.

2.3.3.3 Restoring a File

Perhaps you have deleted the OS/2 kernel or some other important file, and OS/2 will not start. Assuming you have included these elements in a recent ADSM incremental backup, and still using the bootable diskettes, you can restore using this ADSM command:

```
DSMC RESTORE C:\dirname\filename.ext -REPLACE=ALL
```

2.3.3.4 Restoring a Directory

If you have just destroyed an important directory, such as OS2\BOOT, assuming that you have included it in your last ADSM incremental backup, you can restore with this ADSM command:

```
DSMC RESTORE C:\OS2\BOOT\* -REPLACE=ALL
```

2.3.3.5 Restoring an Entire Directory Structure

If an entire directory structure was destroyed because an ill-conceived command such as DELTREE C:\OS2 was issued, assuming you have backed up the structure, you can restore it with this ADSM command:

```
DSMC RESTORE C:\OS2\* -REPLACE=ALL -SUBDIR=YES
```

2.3.3.6 Rebooting the System

After doing any of the above, reboot your system.

2.3.4 If a Test, Verify the Postdisaster Restoration

Before the disaster, and just after the ADSM incremental backup, we listed the contents of the C: drive using the command ″DIR /S /W) and recorded the number of files and bytes. After using the OS/2 bootable technique, and

restoring from the last ADSM backup, we issued the same command again and compared the results to make sure they were the same.

2.3.5 Why Not Bootable Diskettes for an OS/2 ADSM Client with SNA LU 6.2?

We also investigated whether the OS/2 bootable technique would work for an ADSM client that only used SNA for communications with its ADSM server.

Unfortunately, the OS/2 bootable diskette technique does not work with SNA. Because Communications Manager for OS/2 (CM/2) requires the use of OS/2 presentation manager and its associated GUIs, it is not feasible to use bootable diskettes. Even if you start CM/2 from an OS/2 command line, using CMSTART.EXE, you still eventually get to a point where CM/2 expects a desktop to be active.

Here are some ways to deal with APPC recovery:

- If your server can use TCP/IP as well as APPC, the OS/2 bootable diskettes will work regardless of the configuration of the machine being restored (if the appropriate communications card is present). If TCP/IP is packaged on th OS/2 bootable diskettes, the machine can be booted with the OS/2 bootable diskette. Initially use TCP/IP for the ADSM restore, which you then can use to restore the elements for APPC communications with the ADSM server. Of course this assumes that your ADSM server is capable of using TCP/IP even though you have not been using it for communications with that ADSM OS/2 client.
- If you still have another machine on the network that is in APPC communication with the ADSM server, use the CID peer restore method (see Chapter 6, “Recovery of OS/2 and Windows from an OS/2 CID Peer” on page 107) to recover, using NetBIOS to ″see″ the new machine′s drives. You may then reboot using the restored APPC system.

Chapter 3. OS/2 WARP Version 4 Desktop : Bootable, Direct Recovery

In this chapter we explain how to use bootable diskettes to recover a single OS/2 Warp V4 desktop client environment that uses TCP/IP or NetBIOS to communicate with its ADSM server. We review the kind of information to back up in preparation for a disaster, explain how to create bootable diskettes, and discuss how to use the bootable diskettes in conjunction with the saved information to recover after a disaster.

It is also possible to use configuration, installation, and distribution (CID) peer recovery for this platform. Refer to Chapter 6, “Recovery of OS/2 and Windows from an OS/2 CID Peer” on page 107 for information about using CID peer recovery for clients that use Advanced Program-to-Program Communication (APPC) ADSM communications.

We used the gamma version of OS/2 Warp Version 4. We believe that the differences between the gamma and the general availability versions are minimal and they should not cause any difficulties.

3.1 Product Overview

OS/2 Version 4 is a new addition to the IBM family of products. Like its predecessors, OS/2 V4 is an advanced 32-bit operating system. It provides functions such as multitasking and multithreading. It runs 32-bit applications as well as 16-bit DOS and Windows programs. It also provides a variety of networking services such as Internet, office, and remote access.

OS/2 provides two different kinds of file systems: the file allocation table (FAT) file system and the high-performance file system (HPFS). The FAT system is similar to the DOS FAT system. File names are restricted to eight characters with a three-character delimiter. HPFS uses high-speed buffer storage known as cache to provide fast access to large disk volumes. It also supports the coexistence of multiple, active file systems on a single desktop, using multiple, different storage devices. HPFS file names can be as many as 254 characters long.

OS/2 Warp Version 4 is a single-user environment, so security tends to be handled with such mechanisms as lock words. A new function called *security enabling services* provides a new set of APIs for running security applications.

3.2 Predisaster Preparation

This section describes considerations for preparing for a disaster, including ADSM setup and bootable diskette creation.

3.2.1 ADSM Backups

If recovery of the operating system is to be from ADSM, a full backup that includes system files must be taken. This is not the default. The system files will of course be specific to the configuration of the machine being backed up. Figure 12 shows the predisaster normal backups being taken.

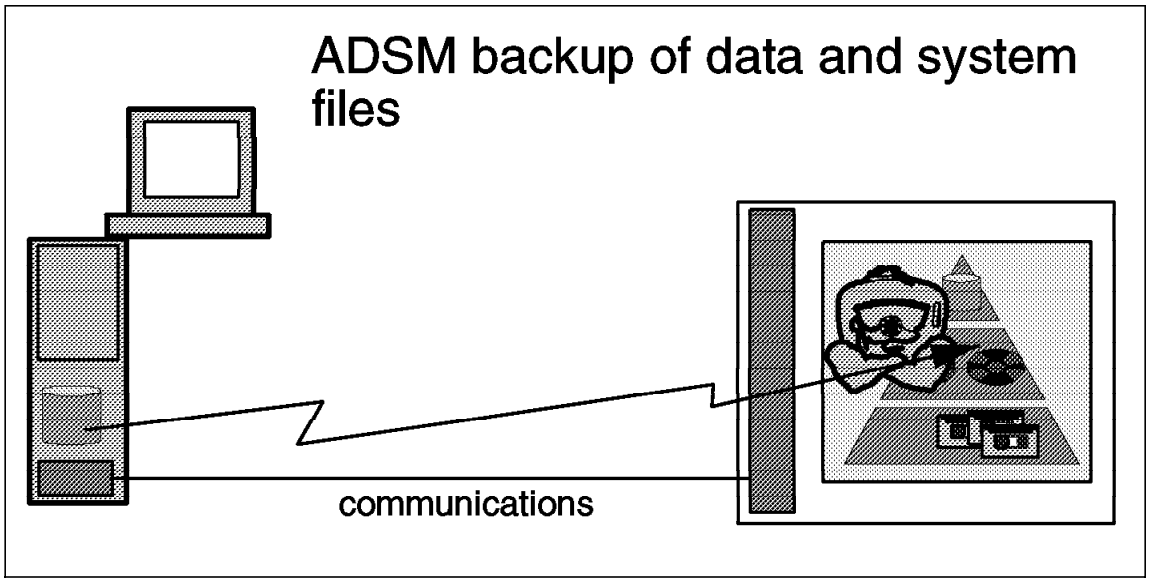


Figure 12. Full ADSM Backup: OS/2 Warp V4

We recommend that you use the following options for the ADSM backup that you will use for the ADSM bare metal restore:

- Set the **Copy Serialization** parameter in the **Backup Copy Group** definition to **Shared Static** This setting allows only those files not being modified to be included in the ADSM backup (preventing a ″fuzzy″ backup). When using this setting, it is best to schedule the ADSM backup during a period of low utilization of the ADSM client. Because this ADSM backup is oriented to provide an image of the workstation to be used in case of disaster, all applications and subsystems running on the machine should be closed before the backup, so that you have the fewest number of open files.
- Because we depend on the existence of an ADSM backup that would provide full restoration of the ADSM client being recovered, we

recommend that the ADSM options file, **DSM.OPT**, only EXCLUDE the SWAPPER.DAT and the EA DATA.SF files. This recommendation implies that you include the operating system software on the C: drive in the ADSM backup. The bootable diskettes will provide only a skeleton version of OS/2 that will enable the ADSM client to function. The assumption is that the newly booted system with the ADSM client will be used to restore the rest of the OS/2 system from an ADSM backup done *for that client.* This may be contrary to your current backup policy (you may currently deliberately EXCLUDE the C: drive from your ADSM backups). This backup should also include empty directories.

3.2.2 Operating Environment of the ADSM Client

In preparation for disaster recovery, we recommend that you collect and save offsite the information listed below in addition to the ADSM backup data. Depending on your installation, you could save this information by using the DRM feature, or you could save it on hardcopy stored offsite. The way in which you save the information is not as important as ensuring that it is saved **somewhere** where it can be easily retrieved along with the client recovery media when a disaster occurs.

- **Hardware configuration**

  Keep information about machine type, bus type, hard disk attachment, and of course, the type of network adapter used. Collect any such information that will help you re-create the hardware setup of the ADSM client that has been destroyed in a disaster. If you are using a PS/2, for instance, you may also include information about where to find copies of the associated PS/2 hardware reference diskettes in case you find yourself needing to replace a hard disk.

- **Partitioning drives**

  Record how the hard drives are partitioned and labeled. You can collect this information by using the Fdisk command. To do the restore, ADSM has to know the hard drive label. We recommend that you define hard drive labels that include the drive letter, to make it easier to determine which ADSM filespace should be restored to which drive at disaster recovery time.

- **Communication details**

  Specific information about your installation communications setup (for example, TCP/IP addresses of the ADSM client and server; SUBNET, ROUTE, and DOMAIN name; and TCP/IP port number of the ADSM service and ADSM node name). This information could be customized on the bootable diskettes. However, if one set of bootable diskettes will be used to service many OS/2 clients, you may want to store this data for each individual client (using offsite hardcopy or DRM).

Optional: Statistics for Postdisaster Recovery Verification

You may want to gather and save information that can be used after a disaster recovery test once the restore process is completed, to validate that all information has indeed been restored correctly. Each installation will have its own ideas about the best way to verify that the recovery is complete. Some possible sources of information for recovery verification are:

- ADSM statistics at the end of the backup, such as the Number of Objects Inspected, would give a tally of the directories and files on the client being backed up.
- CHKDSK command output for each backed up disk

  Run CHKDSK for each drive being backed up and record:

  – *X* number of kilobytes used in *A* number of directories

  – *Y* number of kilobytes used in *B* number of user files

  – *Z* number of kilobytes used in extended attributes

  For FAT drive records:

  – *X* number of kilobytes used in *A* hidden files

  – *Y* number of kilobytes used in *B* number of directories

  – *Z* number of kilobytes used in *C* user files
- DIR command output

  Collect the output of the DIR /A /S command in a file for each drive. After disaster recovery testing, use the output to compare the files available before the test. Utilities such as the AIX DIFF program could be used for this kind of comparison.
- Other test scripts used during your installation's periodic disaster recovery tests.

3.2.3 Creating the Bootable Diskettes

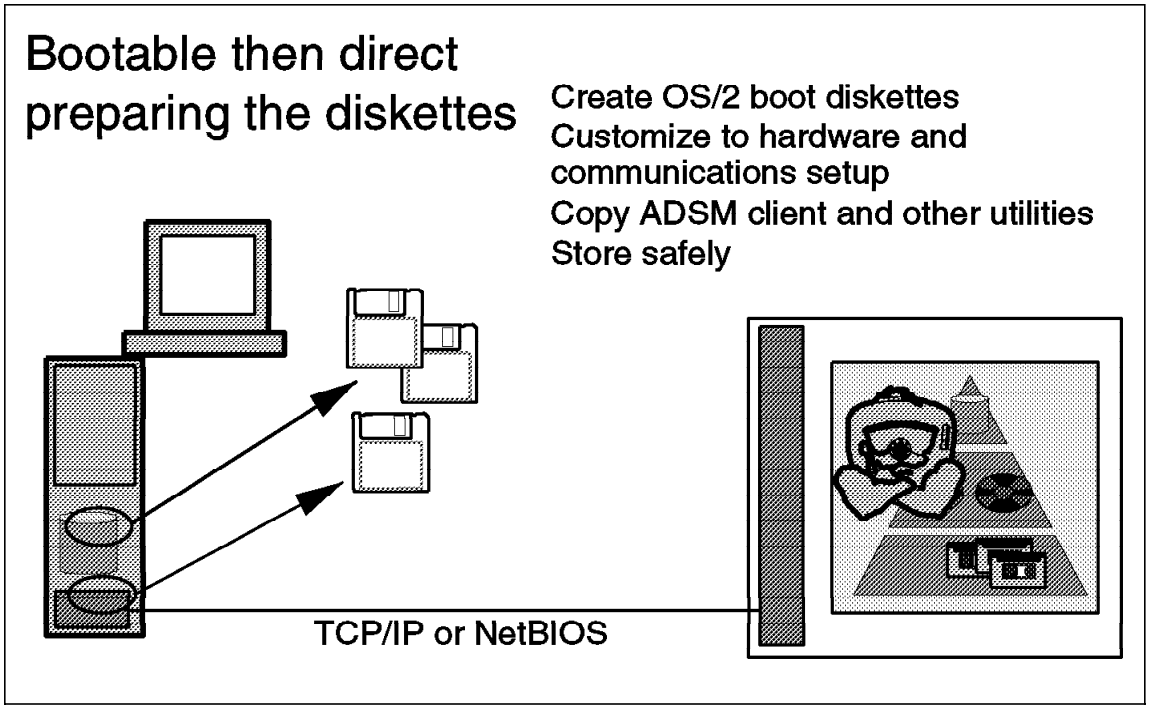


Figure 13. Creating the Bootable Diskettes: OS/2 Warp V4

In this section we describe a method to create bootable diskettes for OS/2 WARP Version 4. The reason for creating these diskettes is that, after a disaster, they can be used to quickly boot a replacement machine with the minimal operating system, communications, and ADSM software necessary to begin file restoration with the ADSM client and server. Normal ADSM recovery can then be used to restore the remainder of the predisaster client environment.

3.2.3.1 Assumptions

Our instructions for creating bootable diskettes apply to OS/2 machines using TCP/IP or NetBIOS with a token ring adapter. We tested only the TCP/IP method but include the NetBIOS instructions as well for your reference. *Modifications may be necessary for this technique to work in environments using other network adapters, hard disk controllers, and so on.*

The instructions apply to the following products:

- OS/2 Warp Version 4.0
- IBM TCP/IP Version 5.1
- ADSM/2 Version 1, Release 2 client code

- ADSM/2 Version 2, Release 1 client code
- Any ADSM server that uses TCP/IP or NetBIOS

A complete ADSM backup as described in 3.2, “Predisaster Preparation” on page 44 should be available at the ADSM server, and the restore should be done to a hardware configuration similar to that of the original ADSM backup/archive client machine.

3.2.3.2 Configuration Used to Test This Technique

We tested the technique on the following configuration:

- Personal Computer 750 with 32 MB of RAM
- 16 Mbps token-ring attachment
- 1.6 GB IDE-attached hard drive, partitioned as follows:
  - C drive: HPFS primary partition, 200 MB, label ″OS2″
- OS/2 Warp Version 4
- IBM TCP/IP Version 5.1 for OS/2 Version 4 (WR08400)
- ADSM/2 Version 2, Release 1, Level 0.3 client code
- ADSM/AIX Version 2, Release 1, Level 0.2 server code

To use this technique you will need:

- Four blank formatted 1.44 MB diskettes
- OS/2 system installation diskettes
- If you are using PS/2 hardware, the associated hardware reference diskettes may be useful.

3.2.3.3 Step-by-Step Instructions

These instructions for creating a set of OS/2 WARP Version 4, TCP/IP or NetBIOS, ADSM/2 client enabled bootable diskettes are based on the method provided by Kenneth Morse of the IBM Washington Systems Center.

Step 1: Create the Base OS/2 Diskettes: Format four 1.44 MB diskettes and label them disk 0, disk 1, disk 2, and disk 3.

Use the Create diskette utility within the OS/2 System folder on the OS/2 WARP Version 4 desktop to create the base OS/2 diskettes. The utility guides you through the creation of the four diskettes.

Disk 0, disk 1, and disk 2 are ready for the next steps. Reformat disk 3 as it will not be set up as you need it to be.

Step 2: Edit Base OS/2 Diskettes by Deleting Files: Remove the following files from disk 2:

```
SYSINST2.EXE
FDISK.COM
```

Step 3: Edit the Base OS/2 Diskettes to Add Files: Once you create the base OS/2 diskettes, add the following files:

- **OS/2 files**

  Below is a list of OS/2 files that you must copy to or create and then copy to disk 1.

Filename	Found in
VDISK.SYS	\OS2\BOOT
OSO0001.MSG	\OS2\SYSTEM
STARTUP.CMD	See B.1, "STARTUP.CMD" on page 271.
FINDRAM.CMD	See B.2, "FINDRAM.CMD" on page 271.
THE.CMD	See B.3, "THE.CMD" on page 272.
PART2.CMD	See B.4, "PART2.CMD" on page 273.
PART3.CMD	See B.5, "PART3.CMD" on page 274.
SETUP.CMD	See B.7, "SETUP.CMD" on page 276.
An editor	- To dynamically choose your settings at boot time, you must have a copy of a tiny editor (for example, TEDIT, which comes with OS/2 Warp). Any editor will do as long as it does not need a graphical interface and fits on the 1.44 MB diskette.

- **LAN Support files**

  You must have the support layer necessary to operate your network card at the hardware level. Following is a list of files which you have to add to disk 2. Next to each filename is a hint as to where to find them on a working LAN attached system.

Filename	Found in
LANMSGEX.EXE	\IBMCOM
PROTOCOL.INI	\IBMCOM
LANMSGDD.OS2	\IBMCOM
PROTMAN.OS2	\IBMCOM
LTO.MSG	\IBMCOM
LANMSGDL.DLL	\IBMCOM\DLL
IBMTOK.OS2	\IBMCOM\MACS
NETBIND.EXE	\IBMCOM\PROTOCOL

  Depending on your setup, you may have to replace IBMTOK.OS2 with whatever NDIS driver is appropriate for your network adapter.

IBMTOK.OS2 works well for most variations of IBM token-ring adapters. For other adapters, you have to determine which NDIS driver you are using. If you do not know which driver you are using, try looking in the following places:

- In PROTOCOL.INI, all of your protocols should be bound to one driver. The internal name of the driver, for example, IBMTOK$, should be awfully close to the file name, for example, IBMTOK.OS2.
- Load up Multi-Protocol Transport Support (MPTS) and look at the driver that is loaded. Many of the driver descriptions list the file name of the driver in parentheses next to the driver's name.
- Look through CONFIG.SYS. Some drivers, such as IBMETHRN.OS2, jump right out at you.

- **TCP/IP files**

  For TCP/IP Version 5.1 support, the following files need to be copied from a working TCP/IP Version 5.1 system to disk 2:

```
Filename      Found in
----------------------
CNTRL.EXE     \MPTN\BIN
IFNDIS.SYS    \MPTN\PROTOCOL
SOCKETS.SYS   \MPTN\PROTOCOL
AFINET.SYS    \MPTN\PROTOCOL
```

- **NetBIOS files**

  For NetBIOS support, the following files need to be copied from a working NetBIOS system to disk 2:

```
Filename      Found in
----------------------
NETBEUI.OS2   \IBMCOM\PROTOCOL
NETBIOS.OS2   \IBMCOM\PROTOCOL
```

Step 4: Modify CONFIG.SYS and CMD Files: Make the following modifications to the CONFIG.SYS file on disk 1:

- **Paths**

  Change the three path statements so that they reference the A: drive:

```
LIBPATH=.;\;A:\;
SET PATH=.;\;A:\;
SET DPATH=.;\;A:\;
```

- **Initialization**

  Ensure that the following lines are included in your CONFIG.SYS:

```
PROTSHELL=SYSINST1.EXE
SET OS2_SHELL=CMD.EXE
```

- **PART2.CMD**

  In the PART2.CMD file on disk 2, change all text occurrences in the PART2.CMD file of *diskette 1* to *diskette 2* and all occurrences of *diskette 2* to *diskette 3.*

- **Device drivers**

  All device drivers copied to disk 2 must be referenced at startup time. Add the following lines to the bottom of CONFIG.SYS. (naturally, include the NetBIOS driver only if you plan to use NetBIOS instead of TCP/IP):

```
REM *** Protocol/LAN/VDISK Drivers ***
DEVICE=\VDISK.SYS 4069,,
DEVICE=\LANMSGDD.OS2 /I:A:\
RUN=\LANMSGEX.EXE
DEVICE=\PROTMAN.OS2 /I:A:\

REM *** Appropriate Network Adapter Driver Here ***
DEVICE=\IBMTOK.OS2

REM *** TCP/IP Version 5.1 Drivers ***
DEVICE=\SOCKETS.SYS
DEVICE=\AFINET.SYS
DEVICE=\IFNDIS.SYS
RUN=\CNTRL.EXE

REM *** NETBIOS DRIVERS * OPTIONAL ***
DEVICE=NETBEUI.OS2
DEVICE=NETBIOS.OS2

REM *** Netbind ***
RUN=\NETBIND.EXE
```

Step 5: Create Disk 3: To create disk 3, you will need a pair of compression-decompression utilities. We mention the use of PKWare′s PKZIP2/PKUNZIP2 and InfoZip′s ZIP/UNZIP, but you can use your favorite compression-decompression utility. Disk 3 will contain compressed versions of the ADSM client, TCP/IP (and/or NetBIOS) files, OS/2 utilities, and a pair of compression and decompression utilities. Here are the steps to create disk 3:

- **Create a temporary directory and collect files**

  To collect all necessary files, create a new directory called, for example, C:\TEMPADSM.

  - **ADSM client files**

Copy the following ADSM files from a working ADSM client to the \TEMPADSM directory you have created:

```
Filename      Found in
-----------------------
DSCAMENG.TXT  \ADSM   - Assuming American English
DSMADMC.EXE   \ADSM   - Only if Administrative Client is required
DSMC.EXE      \ADSM
DSMC.HLP      \ADSM
FCLCNRP.DLL   \ADSM
HPFS386.DLL   \ADSM
NAMPIPES.DLL  \OS2\DLL
```

– **TCP/IP files**

You must copy the following TCP/IP files from your MPTN subdirectory into \TEMPADSM in order to use TCP/IP:

```
Filename      Found in
-----------------------
ARP.EXE       \MPTN\BIN
IFCONFIG.EXE  \MPTN\BIN
ROUTE.EXE     \MPTN\BIN
NETSTAT.EXE   \MPTN\BIN
TCPIPDLL.DLL  \MPTN\DLL
TCPMRI.DLL    \MPTN\DLL
PROTOCOL.     \MPTN\ETC
              (yes, the file Protocol. has no extension)
If there is a need to use the PING utility, then add:
PING.EXE      \MPTN\BIN
TCP32DLL.DLL  \MPTN\DLL
TCPTIME.DLL   \MPTN\DLL
SO32DLL.DLL   \MPTN\DLL
```

– **NetBIOS files**

Copy following file into \TEMPADSM if you are going to use NetBIOS:

```
Filename      Found in
-----------------------
ACSNETB.DLL   \IBMCOM\DLL
```

– **OS/2 utilities**

The following utilities are not required to successfuly run ADSM, but they can come in quite handy, so copy them to \TEMPADSM:

```
Filename      Found in
-----------------------
FDISK.COM     \OS2         - For repartitioning
FORMAT.COM    \OS2         - For reformatting
LABEL.COM     \OS2         - For changing volume names
CHKDSK.COM    \OS2         - For repairing file system damage
ATTRIB.EXE    \OS2         - For altering file attributes
MAKEINI.EXE   \OS2         - For repairing or rebuilding. INI files
XCOPY.EXE     \OS2         - For copying files
INI.RC        \OS2         - Seed file for MAKEINI
INISYS.RC     \OS2         - Seed file for MAKEINI
LOCK.RC       \OS2         - Seed file for MAKEINI
UHPFS.DLL     \OS2\DLL     - For HPFS partition work
SYSINSTX.COM  \ on disk 0  - For bootstrap sector initialization
```

Feel free to include any other small utilities you think may come in handy when working on a damaged system; your only limit is the amount of data that can be compressed to fit on a 1.44 MB diskette.

- **Build the zip file**

  If you use the PkZip2 and PKUnZip2 utilities with C:\TEMPADSM as the temporary directory, execute the following commands to build the zip file on disk 3:

  ```
  C:
  CD C:\TEMPADSM
  PKZIP2 ADSMPACK.ZIP *
  ```

  If you are using the ZIP and UNZIP utilities, execute the following commands to compress all of the files you gathered together into a file named ADSMPACK.ZIP:

  ```
  C:
  CD C:\TEMPADSM
  ZIP ADSMPACK.ZIP *
  ```

  Copy this file to disk 3.

- **Copy the decompression utility**

  Copy the corresponding decompression program (PKUNZIP2.EXE or UNZIP.EXE) to disk 2. If you use InfoZip′s UNZIP.EXE, you will have to copy the NLS.DLL file from your \OS2\DLL subdirectory onto disk 3.

Make sure you edit PART2.CMD on disk 2 and specify which decompression utility you will be using!

3.3 Postdisaster Recovery

In this section we describe how to recover from a disaster to the OS/2 Warp Version 4 ADSM client using the information we saved prior to disaster (described in 3.2, “Predisaster Preparation” on page 44) and the bootable diskettes we created (described in 3.2.3, “Creating the Bootable Diskettes” on page 46.)

To simulate a disaster, we installed a new, blank hard drive on our client machine, so that our machine would no longer boot.

3.3.1 Rebuild Hardware Environment

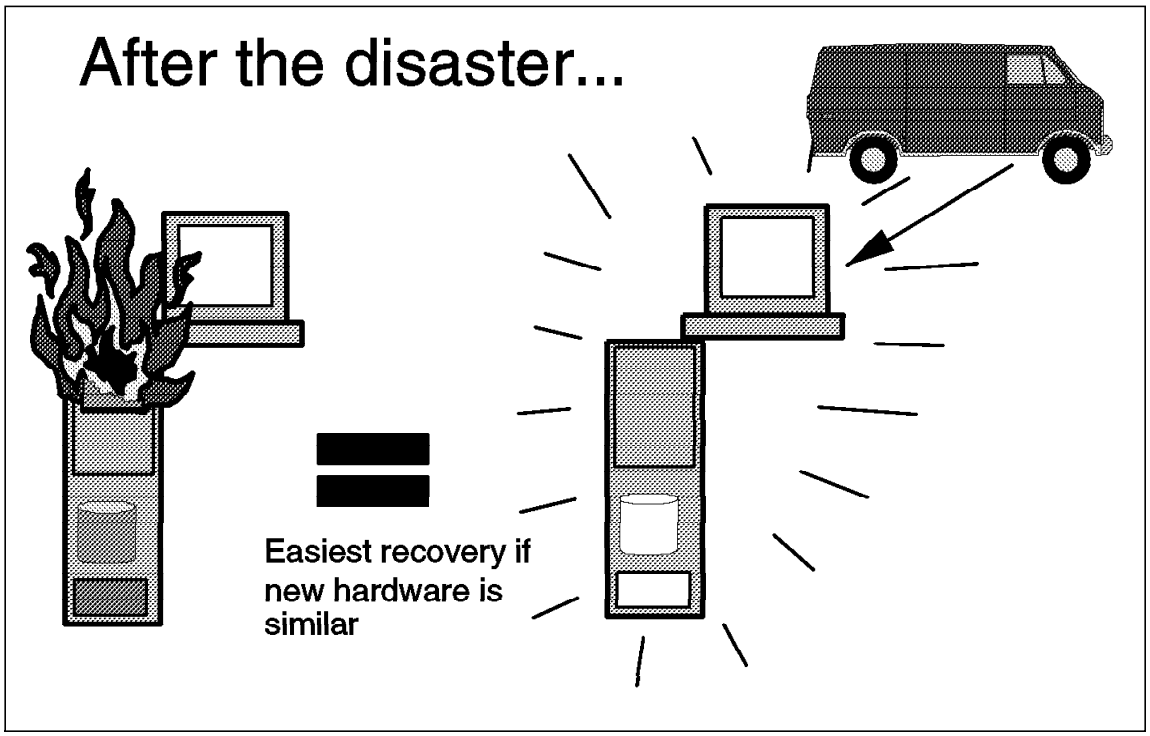


Figure 14. Obtain Suitable Replacement Hardware: OS/2 Warp V4

Retrieve information about the OS/2 machine to help re-create the hardware environment of the destroyed ADSM client. The new replacement machine must have a similar configuration.

If DRM had been used as the repository for this type of information, you can retrieve it by issuing the appropriate ADSM queries to the ADSM server.

For examples of these queries, see 1.3.6, “Disaster Recovery Manager” on page 18.

3.3.2 Boot the Recovery System

Here we describe how the new system is booted from diskettes, how utilities, communications and ADSM are copied to a VDISK and how an ADSM command line client is started ready for the restore.

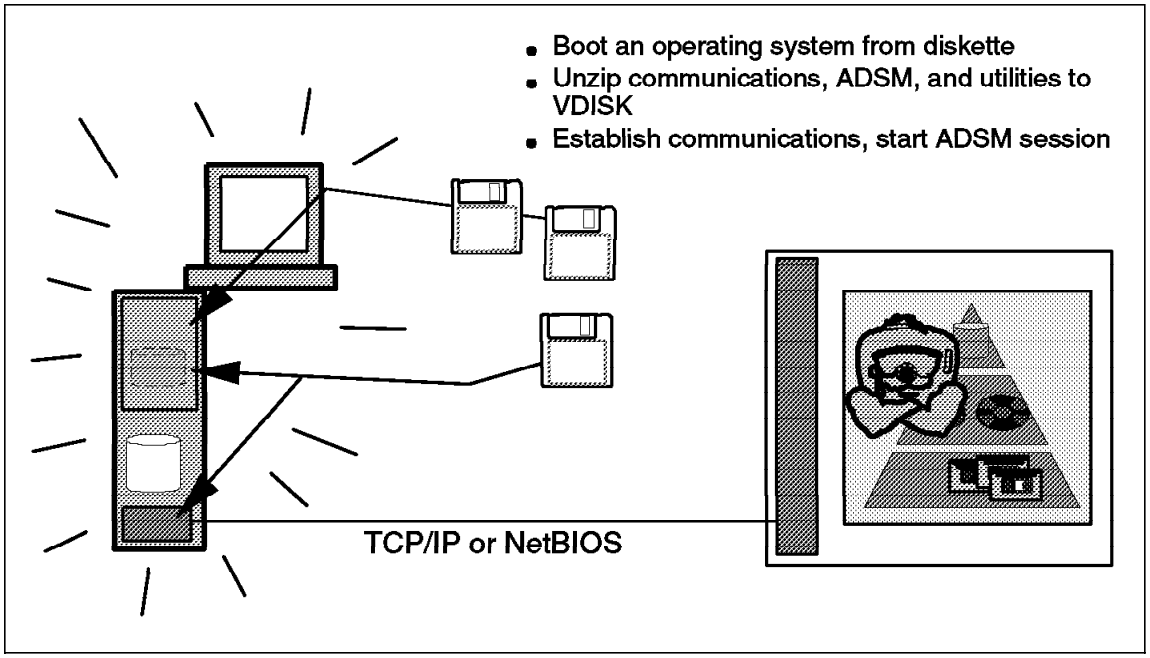


Figure 15. Boot the Diskette System Ready to Recover Warp V4

Use the OS/2 Warp Version 4 bootable diskettes to boot the replacement hardware and prepare for ADSM file recovery. Follow these steps:

- Boot the machine with disk 0, until the blue screen asking for disk 1 appears.
- Insert disk 1 and press <ENTER>.
- Wait for the message asking for disk 2. Insert disk 2 and press <ENTER>. At this point you see on the screen:

```
VDISK version 4 Virtual disk F
disk Size:         4096 KB
Sector Size:       512
Directory Entries: 64
IBM OS/2 LANMSGDD (08/01/96) 5.05 is loaded and operational.
```

Wait for this message and system prompt (be patient):

```
OS/2 Command Interpreter version 4

A:\
```

- Type this command:

  STARTUP.CMD

- Wait for:

```
ADSM BOOTABLE RECOVERY STARTED.........
*********************************************

Searching for a VDISK
VDISK Found as drive (E:\)

Copying files to drive (E:\)

Unpacking file to VDISK
Wait for all diskette activity to stop, (background processes..)
Remove diskette 2 from the drive, and insert diskette 3 and then
Press any key when ready  . . .
```

- Wait for the activity to stop, remove disk 2, insert disk 3, and press <ENTER>.
- Wait for the message requesting disk 2 again:

```
Working...
PKUNZIP (R) FAST!  Extract Utility  Ver. 1.09-OS/2 Prot Mode 1-15-91
Copr. 1989-1991 PKWARE Inc. All Rigths Reserved PKUNZIP/h for help
PKUNZIP Reg. U>S> Pat. an Tm. Off.     IBM LICENSED VERSION


Searching ZIP: A:ADSMPACK.ZIP
  Exploding: UHPFS.DLL
  Exploding: XCOPY.EXE
  .
  .
  .
  Exploding: UHPFS.DLL
  Exploding: XCOPY.EXE
Done...
Please remove diskette 3 from the drive, and insert diskette 2 again and
then
Press any key when ready  . . .
```

- After you remove disk 3, insert disk 2, and press <ENTER>. The tiny editor TEDIT.EXE shows the contents of SETUP.CMD, which contains

ADSM configuration setup information. Normally there is no reason to edit SETUP.CMD unless you are using one set of OS/2 bootable diskettes for several clients and must tailor it to reflect individual machine characteristics. If you have to make changes to SETUP.CMD you can save the changes by pressing F4.

- After the Initialization Complete message appears, the OS/2 prompt appears. At this point you can start the ADSM restore.

```
Configuring ADSM

Configuring ADSM TCP/IP

Configuring TCPIP

Starting TCP/IP
Adding network default, router xxx.xx.xxx.xxx netmask x.x.x.x.

Initialization Complete:  You may now start the ADSM restore...

E:\
```

3.3.3 Restore from the ADSM Backup

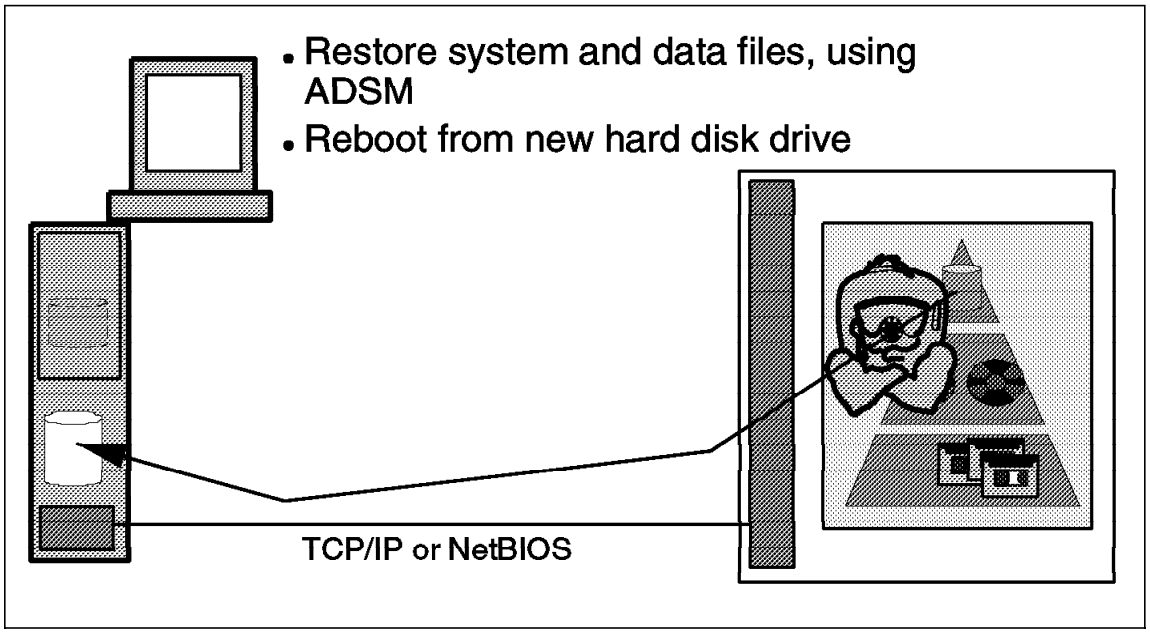


Figure 16. Use the ADSM Command Line Client to Recover the OS/2 Warp Verion 4 Disk(s)

At this point you are ready to begin restoration of files from the ADSM server. Some possible recovery scenarios are described below.

3.3.3.1 Restoring the Whole System

Note: ADSM identifies your drives by their volume name and expects that your replacement drive will have the same setup and label as the original. Use the ADSM QUERY FILESPACE command to find out which volume labels ADSM expects to see.

To restore the whole system from the ADSM backup, invoke the ADSM command line client and issue the following command:

```
RESTORE C:\* -SUBDIR=YES -REPLACE=YES
```

ADSM responds to this command with the following:

```
ADSTAR Distributed Storage Manager
Command Line Backup Client Interface - Version 2, Release 1,Level 0.0
(C) Copyright IBM Corporation, 1990, 1995, All Rigths Reserved.

dsmc> RESTORE C:\* -SUBDIR=YES -REPLACE=YES
RESTORE function invoked.

Please enter password for node "SERVER1": *******

Session established with server ADSM: AIX-RS/6000
  Server Version 2, Release 1, Level 0.2
  Data compression forced on by the server
  Server date/time: 08:30:1996 17:53:11  Last access: 08/30/1996 17:47:55

Restoring            0 C:\TCPCFG.LOG --> C:\TCPCFG.LOG  Done
Restoring          388 C:\AUTOEXEC.01 --> C:\AUTOEXEC.01 . Done
Restoring          368 C:\AUTOEXEC.MGA --> C:\AUTOEXEC.MGA . Done
Restoring        4,278 C:\CONFIG.BK1 --> C:\CONFIG.BK1 . Done
        .          .
        .          .
        .          .
Restore processing finished.
```

3.3.3.2 Restoring the OS/2 Desktop

To restore your OS/2 desktop, use the following commands:

1. Remove the ruined desktop:
   ```
   MOVE C:\DESKTOP \OLDDESK
   ```
2. Restore your saved desktop:
   ```
   DSMC RESTORE C:\DESKTOP\* -SUBDIR=YES
   ```
3. Restore your Desktop program information:
   ```
   DSMC RESTORE C:\OS2\OS2*.INI -REPLACE=ALL
   ```

3.3.3.3 Restoring a File

Perhaps you have deleted the OS/2 kernel or some other important file, and OS/2 will not start. Assuming you have included these elements in a recent ADSM incremental backup, and still using the bootable diskettes, you can restore using this ADSM command:

```
DSMC RESTORE C:\dirname\filename.ext -REPLACE=ALL
```

3.3.3.4 Restoring a Directory

If you have just destroyed an important directory such as OS2\BOOT, assuming that you have included it in your last ADSM incremental backup, you can restore with this ADSM command:

```
DSMC RESTORE C:\OS2\BOOT\* -REPLACE=ALL
```

3.3.3.5 Restoring an Entire Directory Structure

If an entire directory structure was destroyed because an ill-conceived command such as DELTREE C:\OS2 was issued, assuming you have backed up the structure, you can restore it with this ADSM command:

```
DSMC RESTORE C:\OS2\* -REPLACE=ALL -SUBDIR=YES
```

3.3.3.6 Rebooting the System

After doing any of the above, reboot your system.

3.3.3.7 Verify the Postdisaster Restoration

At this point, you would use any statistics you saved with your ADSM backups and bootable diskettes to verify that they are comparable to those you receive after your recovery is complete.

3.3.4 Why Not Bootable Diskettes for an OS/2 ADSM Client with SNA LU 6.2?

We also investigated whether the OS/2 bootable technique would work for an ADSM client that only used SNA for communications with its ADSM server.

Unfortunately, the OS/2 bootable diskette technique does not work with SNA. Because Communications Manager for OS/2 (CM/2) requires the use of OS/2 presentation manager and its associated GUIs, it is not feasible to use bootable diskettes. Even if you start CM/2 from an OS/2 command line, using CMSTART.EXE, you still eventually get to a point where CM/2 expects a desktop to be active.

Here are some ways to deal with APPC recovery:

- If your server can use TCP/IP as well as APPC, the OS/2 bootable diskettes will work regardless of the configuration of the machine being

restored (if the appropriate communications card is present). If TCP/IP is packaged on th OS/2 bootable diskettes, the machine can be booted with the OS/2 bootable diskette. Initially use TCP/IP for the ADSM restore, which you then can use to restore the elements for APPC communications with the ADSM server. Of course this assumes that your ADSM server is capable of using TCP/IP even though you have not been using it for communications with that ADSM OS/2 client.

- If you still have another machine on the network that is in APPC communication with the ADSM server, use the CID peer restore method (see Chapter 6, “Recovery of OS/2 and Windows from an OS/2 CID Peer” on page 107) to recover using NetBIOS to ″see″ the new machine′s drives. You may then reboot using the restored APPC system.

Chapter 4. OS/2 LAN Server: Bootable, Direct Recovery

In this chapter we explain how to use bootable diskettes to recover an OS/2 LAN Server ADSM client environment that uses TCP/IP or NetBIOS to communicate with its ADSM server. We review the kind of information to back up in preparation for a disaster, explain how to create bootable diskettes, and discuss how to use the bootable diskettes in conjunction with the saved information to recover after a disaster.

It is also possible to use configuration, installation, and distribution (CID) peer recovery for this platform. Refer to Chapter 6, “Recovery of OS/2 and Windows from an OS/2 CID Peer” on page 107 for information about using CID peer recovery for clients that use Advanced Program-to-Program Communication (APPC) ADSM communications.

4.1 Product Overview

The **IBM OS/2 LAN Server** is a network operating system that provides comprehensive LAN capabilities to interconnected workstations on PC networks.

4.1.1 OS/2 LAN Server Entry

LAN Server Entry provides:

- Resource sharing for files and directories (data areas), OS/2 applications, Windows and DOS applications, printers, and serial devices.
- Support for *multiple requesters* including OS/2, Windows, DOS, MicroSoft LAN Manager, Macintosh Appleware, Windows Version 4 Workgroups, and Windows NT.
- Support for FAT and HPFS file systems
- Access control profiles (ACPs) to define security permissions for LAN resources. Access to a LAN resource can be defined for a user, groups of users, or on a universal access level.
- Remote initial program load (IPL) to enable medialess systems without a requester installed to access the code required to IPL and use the services on the network. OS/2, Windows, and DOS requesters can be IPL′d remotely.
- Messaging: LAN Server requesters have a messaging service that allows simple messages to be sent to and received by other users on the network.

- Communications methods: NetBIOS, TCP/IP, NetBIOS over TCP/IP, IPX/SPX, and IEEE 802.2 are provided by the MPTS component of OS/2 LAN Server.

4.1.2 OS/2 LAN Server Advanced

In addition to the function that OS/2 LAN Server Entry provides, OS/2 LAN Server Advanced provides support for:

- The 386-HPFS, which provides improved performance over the FAT and HPFS. 386-HPFS has extremely fast access to very large disk volumes and optimizes server performance when many files are open simultaneously. 386-HPFS allows directory level management of disk space by setting limits defining the maximum size to which a particular directory can grow. *Local security* for the 386-HPFS extends security with access restrictions for users working locally at the server.
- Symmetric multiprocessing, which enables OS/2 LAN Server Advanced to be run on symmetrical multiprocessor (SMP) hardware with two, four, or eight processors.
- Fault tolerance, which protects against disk failures by providing disk mirroring and duplexing, fault monitoring and reporting, and error correction and support for hot-swappable disks in a disk array.

4.2 Predisaster Preparation

The disaster we are preparing for is the total and catastrophic loss of the ADSM client, where provision has to be made to restore everything from the bare metal up. If our disaster recovery preparations can cover this worst case scenario, we can assume that they will also be able to handle recovery from lesser disasters.

In this section we discuss the information to collect and save before a disaster to enable a bare metal restore.

4.2.1 ADSM Backups

If recovery of the operating system is to be from ADSM, a full backup that includes system files must be taken. This is not the default. The system files will of course be specific to the configuration of the machine being backed up. Figure 17 on page 63 shows the predisaster normal backups being taken.

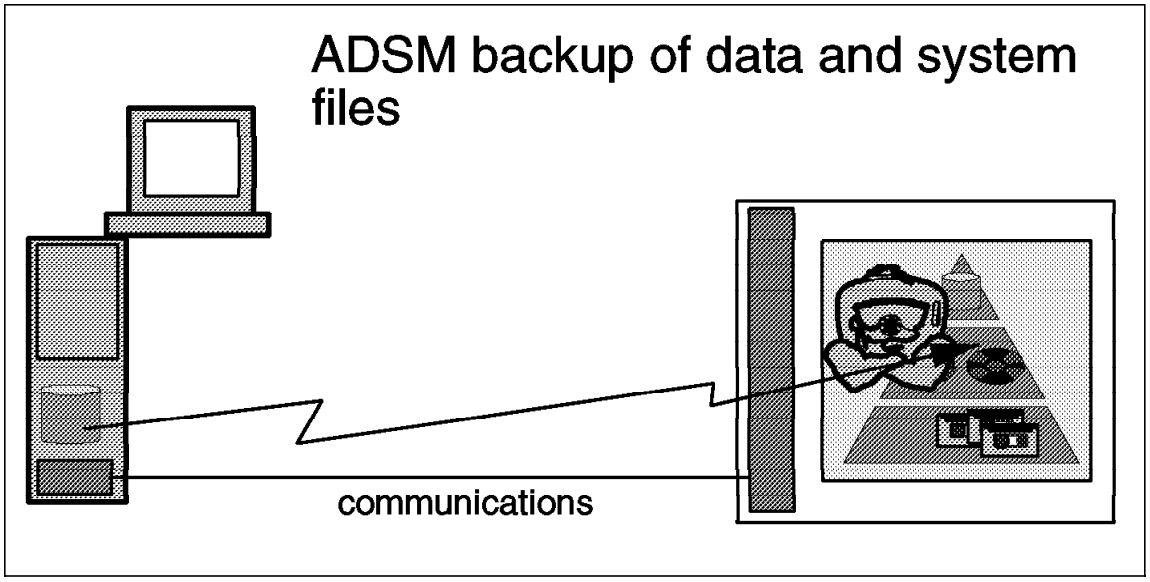


Figure 17. Full ADSM Backup of OS/2 LAN Server System and Data Files

We recommend that you use the following options for the ADSM backup that you will use for the ADSM bare metal restore:

- Set the **Copy Serialization** parameter in the **Backup Copy Group** definition to **Shared Static** This setting allows only those files not being modified to be included in the ADSM backup (preventing a ″fuzzy″ backup). When using this setting, it is best to schedule the ADSM backup during a period of low utilization of the ADSM client. Because this ADSM backup is oriented to provide an image of the workstation to be used in case of disaster, all applications and subsystems running on the machine should be closed before the backup, so that you have the fewest number of open files.
- Because we depend on the existence of an ADSM backup that would provide full restoration of the ADSM client being recovered, we recommend that the ADSM options file, **DSM.OPT**, only EXCLUDE the SWAPPER.DAT and the EA DATA.SF files. This recommendation implies that you include the operating system software on the C: drive in the ADSM backup. The bootable diskettes will provide only a skeleton version of OS/2 that will enable the ADSM client to function. The assumption is that the newly booted system with the ADSM client will be used to restore the rest of the OS/2 system from an ADSM backup done *for that client.* This may be contrary to your current backup policy (you may currently deliberately EXCLUDE the C: drive from your ADSM backups). This backup should also include empty directories.

- Complete at least one incremental ADSM backup to capture any empty directories. The domain control database (DCDB) may have empty directories if you do not have external serial devices, files, or printer resources. OS/2 LAN Server will attempt to use them at startup and will fail if they are not found.
- Back up the ACPs, which protect access to files and directories. Here is an overview of the steps required to back up the ACPs:

  1. Use the OS/2 LAN Server BACKACC utility to produce a list of the ACPs in a file that ADSM can back up. The BACKACC utility copies the NET.ACC file containing server-unique information, LAN userids, group IDs, passwords, and all of the ACPs (if OS/2 LAN Server Entry) or all of the ACPs except those of the files and directories in the 386-HPFS (if OS/2 LAN Server Advanced). If you are using the OS/2 LAN Server Advanced 386-HPFS, for each drive BACKACC will backup the ACPs for the files and directories in an additional file called ACLBAKx.ACL, where x is the drive letter. In this case, you must use the BACKACC command once for each drive.
  2. Run the BACKACC.EXE utility to back up the NET.AUD file containing audit log information for the server. Here are the commands you can use to run BACKACC.EXE against the C and D drives:

     ```
     BACKACC C:\ /S /V
     BACKACC D:\ /S /V
     ```

     The NET.ACC file will be copied to:

     ```
     C:\IBMLAN\ACCOUNTS\NETACC.BKP
     ```

     The NET.AUD file will be copied to:

     ```
     C:\IBMLAN\ACCOUNTS\NETAUD.BKP
     ```

     The access control list will be copied to:

     ```
     C:\IBMLAN\ACCOUNTS\ACLBAKC.ACL: and
     C:\IBMLAN\ACCOUNTS\ACLBAKD.ACL: files.
     ```

     Here is the output from the commands:

```
C:\backacc c:\ /s /v

Successfully backed up NET.ACC to NETACC.BKP.
Successfully backed up NET.AUD to NETAUD.BKP.
Access Control List backup file is C:\IBMLAN\ACCOUNTS\ACLBAKC.ACL.
Backing up Access Control Lists .....

Backing up Access Control Lists for: C:\IBMLAN\DCDB\FILES
Backing up Access Control Lists for: C:\IBMLAN\DCDB\PRINTERS
Backing up Access Control Lists for: C:\IBMLAN\DCDB\USERS\USER01
Backing up Access Control Lists for: C:\IBMLAN\DCDB\USERS\USER01\BATCH
Backing up Access Control Lists for: C:\IBMLAN\REPL\IMPORT\SCRIPTS

BACKACC completed successfully.
C:\


C:\backacc D:\ /s /v

Successfully backed up NET.ACC to NETACC.BKP.
Successfully backed up NET.AUD to NETAUD.BKP.
Access Control List backup file is C:\IBMLAN\ACCOUNTS\ACLBAKD.ACL.
Backing up Access Control Lists .....

Backing up Access Control Lists for: D:\PGM1
BACKACC completed successfully.
C:\
```

- OS/2 LAN Server Advanced does not provide a utility to back up the directory size limits. A method for doing so through the LAN Server API is described in *Using ADSM to Back Up OS/2 LAN Server and WARP Server,* SG24-4682.

4.2.2 Operating Environment of the ADSM Client

In preparation for disaster recovery we recommend that you collect and save offsite the information listed below in addition to the ADSM backup data. Depending on your installation, you could save this information by using the DRM feature, or you could save it on hardcopy stored offsite. The way in which you save the information is not as important as ensuring that it is saved **somewhere** where it can be easily retrieved along with the client recovery media when a disaster occurs.

- **Hardware configuration**

  Keep information about machine type, bus type, hard disk attachment, and of course, the type of network adapter used. Collect any such information that will help you re-create the hardware setup of the ADSM client that has been destroyed in a disaster. If you are using a PS/2, for instance, you may also include information about where to find copies of the associated PS/2 hardware reference diskettes in case you find yourself needing to replace a hard disk.

- **Partitioning drives**

Record how the hard drives are partitioned and labeled. You can collect this information by using the Fdisk command. To do the restore ADSM has to know the hard drive label. We recommend that you define hard drive labels that include the drive letter, to make it easier to determine which ADSM filespace should be restored to which drive at disaster recovery time.

- **Communication details**

  Specific information about your installation communications setup (for example, TCP/IP addresses of the ADSM client and server; SUBNET, ROUTE, and DOMAIN name; TCP/IP port number of the ADSM service; and ADSM node name). This information could be customized on the bootable diskettes. However, if one set of bootable diskettes will be used to service many OS/2 clients, you may want to store this data for each individual client (using offsite hardcopy or DRM).

For more information about ADSM backups, have a look at *Using ADSM to Back Up OS/2 Lan Server and Warp Server* SG24-4682.

Optional: Statistics for Postdisaster Recovery Verification

You may want to gather and save information that can be used after a disaster recovery test once the restore process is completed, to validate that all information has indeed been restored correctly. Each installation will have its own ideas about the best way to verify that the recovery is complete. Some possible sources of information for recovery verification are:

- ADSM statistics at the end of the backup, such as the Number of Objects Inspected, would give a tally of the directories and files on the client being backed up.
- CHKDSK command output for each backed up disk

  Run CHKDSK for each drive being backed up and record:

  – *X* number of kilobytes used in *A* number of directories

  – *Y* number of kilobytes used in *B* number of user files

  – *Z* number of kilobytes used in extended attributes

  For FAT drive records:

  – *X* number of kilobytes used in *A* hidden files

  – *Y* number of kilobytes used in *B* number of directories

  – *Z* number of kilobytes used in *C* user files
- DIR command output

  Collect the output of the DIR /A /S command in a file for each drive. After disaster recovery testing, use the output to compare the files available before the test. Utilities such as the AIX DIFF program could be used for this kind of comparison.
- Other test scripts used during your installation′s periodic disaster recovery tests.

4.2.3 Creating the Bootable Diskettes

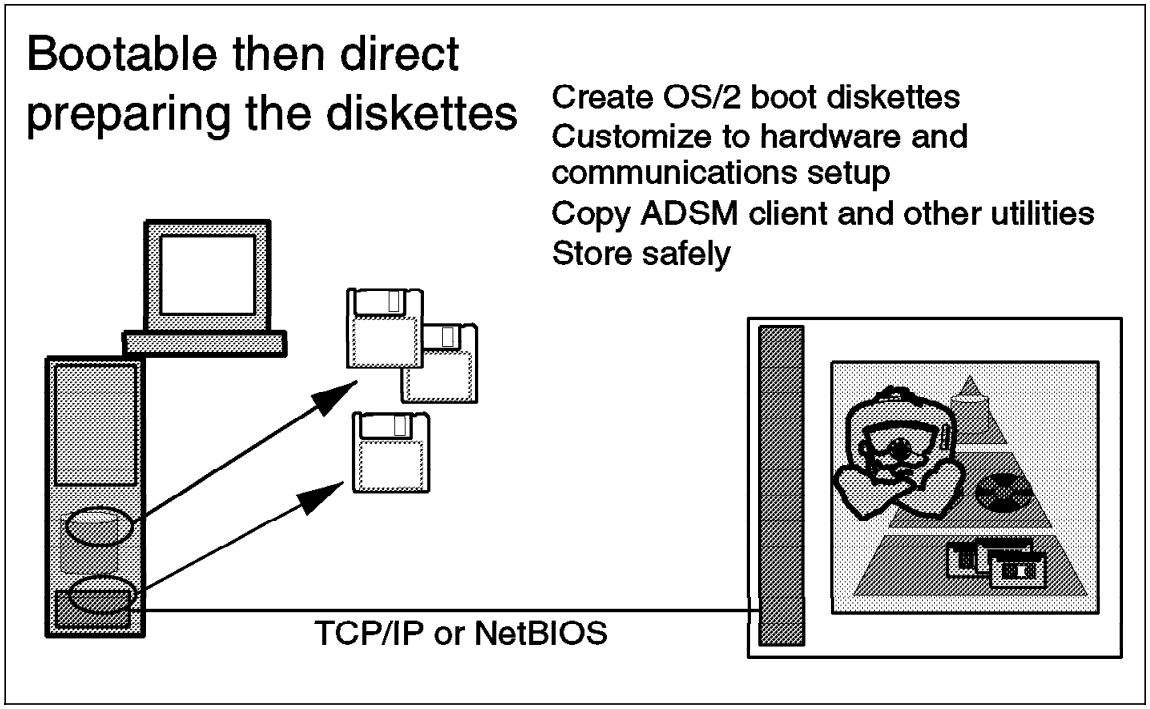


Figure 18. Creating the Bootable Diskettes for OS/2 LAN Server

In this section we describe a technique for creating bootable diskettes for OS/2 LAN Server Advanced Version 4. After a disaster, you use these diskettes to quickly boot a replacement machine with the minimal operating system, communications, and ADSM software necessary to begin file restoration with the ADSM client and server. Normal ADSM recovery can then be used to recover the remainder of the predisaster client environment.

4.2.3.1 Assumptions

Our instructions for creating bootable diskettes apply to machines running OS/2, using TCP/IP or NetBIOS with a token ring adapter. We tested only the TCP/IP method but include the NetBIOS instructions as well for your reference. *Modifications may be necessary for this technique to work in environments using other network adapters, hard disk controllers, and so on.*

The instructions apply to the following products:

- OS/2 LAN Server Advanced Version 4.00
- IBM TCP/IP V3.0
- ADSM/2 Version 1, Release 2 client code
- ADSM/2 Version 2, Release 1 client code

- Any ADSM server that uses TCP/IP or NetBIOS

A complete ADSM backup as we describe in 4.2, “Predisaster Preparation” on page 62 should be available at the ADSM server, and the restore should be done to a hardware configuration similar to that of the original ADSM backup/archive client machine.

4.2.3.2 Configuration Used to Test This Technique

We tested this technique on the following configuration:

- Personal Computer 750 with 32 MB of RAM
- 16 Mbps token-ring attachment
- 1.6 GB IDE-attached hard drive, partitioned as follows:
  - C drive: HPFS primary partition, 200 MB, label ″OS2″
  - D drive: HPFS logical drive, 1450 MB, label ″PROJECT″
- OS/2 WARP Version 3.0
- OS/2 WARP Connect with WIN-OS2 Version 3.00
- IBM OS/2 LAN Server Advanced Version 4.00
- IBM TCP/IP Version 3.0 for OS/2 Version 3.00
- 386-HPFS
- ADSM/2 Version 2, Release 1, Level 0.3 client code
- ADSM/AIX Version 2, Release 1, Level 0.2 server code

To use this technique you will need:

- Three blank formatted 1.44 MB diskettes
- OS/2 system installation diskettes
- If you are using PS/2 hardware, the associated hardware reference diskettes may be useful.

4.2.3.3 Step-by-Step Instructions

These instructions for creating a set of OS/2 LAN Server Advanced Version 4, TCP/IP or NetBIOS, ADSM/2 client enabled diskettes are based on the method provided by Kenneth Morse of the IBM Washington Systems Center. Modifications were made to allow usage of 386-HPFS used by OS/2 LAN Server Advanced.

Step 1: Create the Base OS/2 Diskettes: Format three 1.44 MB diskettes and label them disk 0, disk 1 and disk 2. Make a DISKCOPY of OS/2 installation diskettes disk 0 and disk 1. Disk 0 is ready to use.

Step 2: Edit Base OS/2 Diskettes by Deleting Files: Remove the following files from disk 1:

```
OS2LOGO.
BUNDLE.
FDISK.COM
SYSINST2.EXE
XDFLOPPY.FLT
DEL.LST
MOUSE.SYS
HPFS.IFS
SIPANEL1.DLL
SYSLEVEL.OS2
```

Step 3: Edit the Base OS/2 Diskettes to Add Files: Once you create the base OS/2 diskettes, some changes have to be made to them:

- **OS/2 files**

  Below is a list of OS/2 files that you must copy to or create and then copy to disk 1.

Filename	Found in
VDISK.SYS	\OS2\BOOT
NLS.DLL	\OS2\DLL
STARTUP.CMD	See B.1, "STARTUP.CMD" on page 271.
FINDRAM.CMD	See B.2, "FINDRAM.CMD" on page 271.
THE.CMD	See B.3, "THE.CMD" on page 272.
PART2.CMD	See B.4, "PART2.CMD" on page 273.
PART3.CMD	See B.5, "PART3.CMD" on page 274.
SETUP.CMD	See B.7, "SETUP.CMD" on page 276.
TEDIT.EXE	\OS2

- **LAN support files**

  You must have the support layer necessary to operate your network card at the hardware level. Below is a list of files that you have to add to disk 1. Next to each file name is a hint as to where to find it on a working LAN-attached system.

Filename	Found in
LANMSGEX.EXE	\IBMCOM
PROTOCOL.INI	\IBMCOM
LANMSGDD.OS2	\IBMCOM
PROTMAN.OS2	\IBMCOM
LTO.MSG	\IBMCOM
LT2.MSG	\IBMCOM
PRO.MSG	\IBMCOM
LANMSGDL.DLL	\IBMCOM\DLL

```
IBMTOK.OS2    \IBMCOM\MACS
NETBIND.EXE   \IBMCOM\PROTOCOL
```

- **TCP/IP files**

  For TCP/IP Version 3.0 support, the following files have to be copied from a working TCP/IP Version 3.0 system to disk 1:

```
Filename      Found in
----------------------
CNTRL.EXE     \MPTN\BIN
IFNDIS.SYS    \MPTN\PROTOCOL
SOCKETS.SYS   \MPTN\PROTOCOL
AFINET.SYS    \MPTN\PROTOCOL
```

- **NetBIOS files**

  For NetBIOS support, the following files have to be copied from a working NetBIOS system to disk 1:

```
Filename      Found in
----------------------
NETBEUI.OS2   \IBMCOM\PROTOCOL
NETBIOS.OS2   \IBMCOM\PROTOCOL
```

- **386-HPFS files**

  Add the following files to disk 1:

```
Filename      Found in
----------------------
386-HPFS.IFS  \IBM386FS
386-HPFS.INI  \IBM386FS
HFS.MSG       \IBM386FS
BOOTSH.EXE    \IBM386FS
BSH.MSG       \IBM386FS
BSHH.MSG      \IBM386FS
```

Step 4: Modify CONFIG.SYS and CMD Files:

Make the following modifications to the CONFIG.SYS file on disk 1:

- **Resolve references on CONFIG.SYS**

  Remove any CONFIG.SYS references to the following files:

```
XDFLOPPY.FLT
MOUSE.SYS
```

- **Paths**

  The three path statements have to be changed so that they reference the A: drive:

```
LIBPATH=.;\;A:\;
SET PATH=.;\;A:\;
SET DPATH=.;\;A:\;
```

- **Initialization**

  To correctly install 386-HPFS and execute the STARTUP.CMD, include the following lines in your CONFIG.SYS:

  ```
  PROTSHELL=BOOTSH.EXE CMD.EXE /K STARTUP.CMD
  IFS=386-HPFS.IFS A:\386-HPFS.INI /AUTOCHECK:*
  SET OS2_SHELL=CMD.EXE
  ```

  Note on HPFS Only

  If you are using HPFS to correctly execute the STARTUP.CMD, include the following lines in your CONFIG.SYS file:

  ```
  PROTSHELL=SYSINST1.EXE
  SET OS2_SHELL=CMD.EXE
  ```

- **Device drivers**

  All device drivers copied to disk 1 need to be referenced at startup time. Add the following lines to the bottom of CONFIG.SYS (we only used the TCP/IP driver-you should only include the NetBIOS driver below if you plan to use NetBIOS instead of TCP/IP):

  ```
  REM *** Protocol/LAN/VDISK Drivers ***
  DEVICE=\VDISK.SYS 4069,,
  DEVICE=\LANMSGDD.OS2 /I:A:\
  RUN=\LANMSGEX.EXE
  DEVICE=\PROTMAN.OS2 /I:A:\

  REM *** Appropriate Network Adapter Driver Here ***
  DEVICE=\IBMTOK.OS2

  REM *** TCP/IP Version 3.0 Drivers ***
  DEVICE=\SOCKETS.SYS
  DEVICE=\AFINET.SYS
  DEVICE=\IFNDIS.SYS
  RUN=\CNTRL.EXE

  REM *** NETBIOS DRIVERS * OPTIONAL ***
  DEVICE=NETBEUI.OS2
  DEVICE=NETBIOS.OS2

  REM *** Netbind ***
  RUN=\NETBIND.EXE
  ```

Step 5: Create Disk 2: To create disk 2, you will need a pair of compression-decompression utilities. We mention the use of PKWare's PKZIP2/PKUNZIP2 and InfoZip's ZIP/UNZIP but you can use your favorite compression-decompression utility. Disk 3 will contain compressed versions of the ADSM client, TCP/IP (and/or NetBIOS) files, OS/2 utilities, and an appropriate decompression utility.

- **Create a temporary directory**

  To collect all necessary files, create a new directory called, for example C:\TEMPADSM. Switch to C:\ and issue:

  ```
  MD TEMPADSM
  ```

- **ADSM client files**

  Copy the following ADSM files from a working ADSM client to the \TEMPADSM directory you've created:

  ```
  Filename      Found in
  ------------------------
  DSCAMENG.TXT  \ADSM   - Assuming American English
  DSMADMC.EXE   \ADSM   - Only if Administrative Client is required
  DSMC.EXE      \ADSM
  DSMC.HLP      \ADSM
  FCLCNRP.DLL   \ADSM
  HPFS386.DLL   \ADSM
  NAMPIPES.DLL  \OS2\DLL
  ```

- **TCP/IP files**

  You will need the following TCP/IP files from your TCPIP or MPTN subdirectories copied into \TEMPADSM in order to use TCP/IP:

  ```
  Filename      Found in
  ------------------------
  ARP.EXE       \MPTN\BIN
  IFCONFIG.EXE  \MPTN\BIN
  PING.EXE      \MPTN\BIN
  ROUTE.EXE     \MPTN\BIN
  NETSTAT.EXE   \MPTN\BIN
  TCPIPDLL.DLL  \MPTN\DLL or \TCPIP\DLL
  PROTOCOL.     \MPTN\ETC or \TCPIP\ETC
                (The file Protocol. has no extension)
  ```

- **NetBIOS files**

  To support NetBIOS you will need the following file, so copy it into \TEMPADSM if you are going to use NetBIOS:

  ```
  Filename      Found in
  ------------------------
  ACSNETB.DLL   \IBMCOM\DLL
  ```

- **OS/2 utilities**

  The following are by no means required for a successful running of ADSM but you may find that they come in quite handy, so you should add these files to your \TEMPADSM subdirectory as well:

```
Filename      Found in
-----------------------
FDISK.COM     \OS2     - For repartitioning if necessary
FORMAT.COM    \OS2     - For reformatting if necessary
LABEL.COM     \OS2     - For changing volume names
CHKDSK.COM    \OS2     - For repairing filesystem damage
ATTRIB.EXE    \OS2     - For altering file attributes
MAKEINI.EXE   \OS2     - For repairing/rebuilding .INI files
XCOPY.EXE     \OS2     - For copying files
INI.RC        \OS2     - Seed file for MAKEINI
INISYS.RC     \OS2     - Seed file for MAKEINI
LOCK.RC       \OS2     - Seed file for MAKEINI
NETSTAT.EXE   \OS2     - For checking the network
SYSINSTX.COM  \OS2     - For bootstrap sector initialization
UHPFS.DLL     \OS2\DLL - For HPFS partition work
OS0001.MSG    \OS2\SYSTEM - OS/2 Message repository.
```

OS0001.MSG

Because of space restrictions we did not put this file on disk 1. This is the stock OS/2 message file. When you finally use the diskettes to boot OS/2 LAN Services, you will get a message stating that the operating system could not find message 1467. If you were to type HELP SYS1467 on a different machine, you would see:

```
SYS1467:  VDISK Version 2.1 Virtual disk ***
disk Size:          *** KB
Sector Size:        ***
Directory Entries:  ***
```

In other words, don't worry about it!

- **Build the zip file**

  If you use the PkZip2 and PKUnZip2 utilities with C:\TEMPADSM as the temporary directory, execute the following commands to build the zip file on disk 2:

```
C:
CD C:\TEMPADSM
PKZIP2 ADSMPACK.ZIP *
```

If you are using the ZIP and UNZIP utilities, execute the following commands to compress all of the files you gathered together into a file named ADSMPACK.ZIP.

```
C:
CD C:\TEMPADSM
ZIP ADSMPACK.ZIP *
```

Copy this file to disk 2.

- **Copy the decompression Utility**

  Copy the corresponding decompression program (PKUNZIP2.EXE or UNZIP.EXE) to disk 2. If you use InfoZip′s UNZIP.EXE, you will have to copy the NLS.DLL file from your \OS2\DLL subdirectory onto disk 2.

Make sure you edit PART2.CMD on disk 1 and specify which decompression utility you will be using!

4.3 Post Disaster Recovery

In this section we describe how to recover from a disaster to the OS/2 LAN Server Advanced Version 4 ADSM client by using the information you saved before the disaster (described in 4.2, “Predisaster Preparation” on page 62) and the bootable diskettes you created (described in 4.2.3, “Creating the Bootable Diskettes” on page 67).

To simulate a disaster, we reformatted the C: and D: drives so that the machine would no longer boot.

To recover, we rebuilt the hardware environment, booted the recovery system, and restored from the ADSM backup.

4.3.1 Rebuild the Hardware Environment

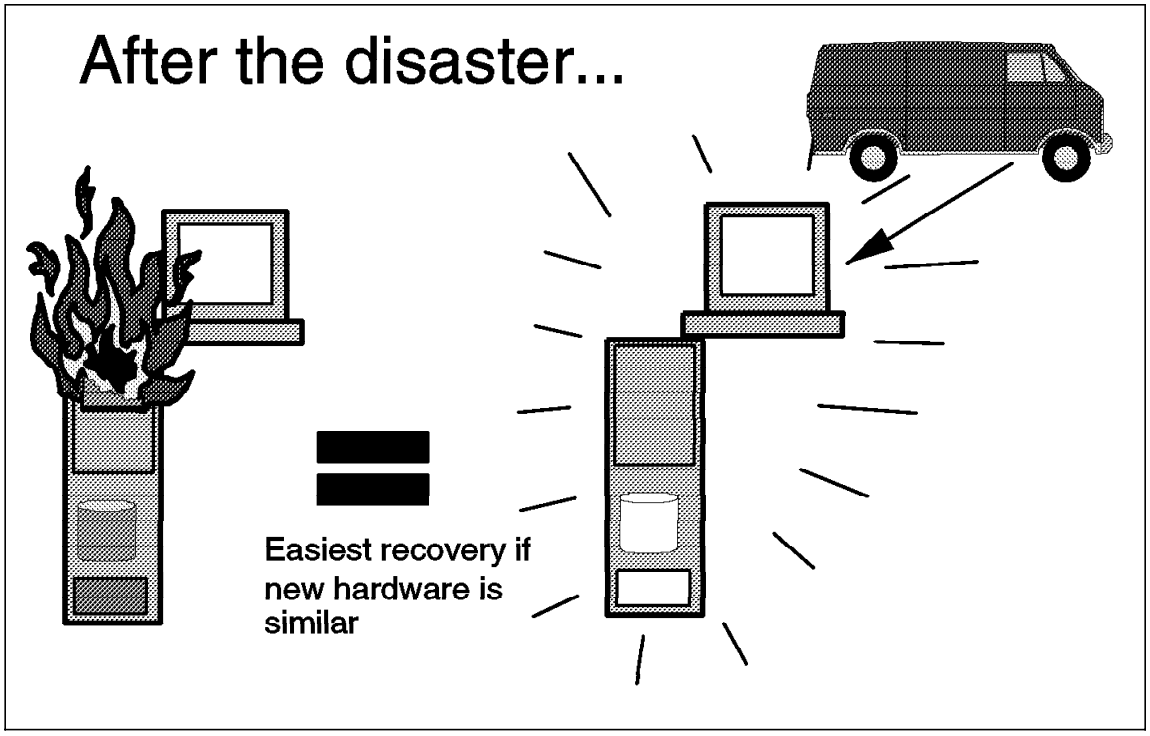


Figure 19. Re-creating the Hardware Environment: OS/2 LAN Server

Retrieve information about the OS/2 LAN Server machine to help re-create the hardware environment of the destroyed ADSM client. The new replacement machine must have a similar configuration see Figure 19

If DRM had been used as the repository for this type of information, you can retrieve it by issuing the appropriate ADSM queries to the ADSM server. For examples of these queries, see 1.3.6, “Disaster Recovery Manager” on page 18.

4.3.2 Boot the Recovery System

Use the OS/2 LAN Server Version 4 bootable diskettes to boot the replacement hardware and prepare for ADSM file recovery. Follow these steps:

1. Boot the machine with disk 0, until the blue screen asking for disk 1 appears.
2. Insert disk 1 and press <ENTER>. Wait for the message asking for disk 2. At this point you see on the screen:

```
The 386 HPFS file  system driver is installed
SYS0318: Message file OS0001.MSG cannot be found for message  1467.

IBM OS/2 LANMSGDD ( 04/26/95 ) 2.01 is loaded and operational.
IBM OS/2 LAN Protocol Manager

ADSM BOOTABLE RECOVERY STARTED........
*********************************************

Searching for a VDISK
VDISK Found as drive (E:\)

Copying files to drive (E:\)

Unpacking file to VDISK
Wait for all diskette activity to stop, (background processes..)
Remove diskette 1 from the drive, and insert diskette 2 and then
Press any key when ready  . . .
```

Message SYS0318

The SYS0318 message reports that a repository file is not available to retrieve the contents of message 1467. The format of message 1467 is:

```
SYS1467: VDISK Version 2.1 Virtual disk ***
disk Size:          4000 KB
Sector Size:        512
Directory Entries:  64
```

3. Wait for the activity to stop, remove disk 1, insert disk 2 and press <ENTER>. Wait for the message requesting disk 1 again:

```
Working...
PKUNZIP (R) FAST!  Extract Utility  Ver. 1.09-OS/2 Prot Mode 1-15-91
Copr. 1989-1991 PKWARE Inc. All Rights Reserved PKUNZIP/h for help
PKUNZIP Reg. U>S> Pat. an Tm. Off.     IBM LICENSED VERSION


Searching ZIP: A:ADSMPACK.ZIP
  Exploding: UHPFS.DLL
  Exploding: XCOPY.EXE
  .
  .
  .
  Exploding: UHPFS.DLL
  Exploding: XCOPY.EXE
Done...
Please remove diskette 2 from the drive, and insert diskette 1 and then
Press any key when ready  . . .
```

4. After you remove disk 2, insert disk 1, and press <ENTER>, the tiny editor TEDIT.EXE shows the contents of SETUP.CMD, which contains ADSM configuration setup information. Normally there is no reason to edit SETUP.CMD unless you are using one set of OS/2 bootable diskettes for several clients and must tailor it to reflect individual machine characteristics. If you have to make changes to SETUP.CMD, you can save the changes by pressing F4.
5. After the Initialization Complete message appears, the OS/2 prompt appears. At this point you can start the ADSM restore.

```
Configuring ADSM

Configuring ADSM TCP/IP

Configuring TCPIP

Starting TCP/IP

Initialization Complete:  You may now start the ADSM restore...

E:\
```

4.3.3 Set Up a New Hard Drive

The nature of our "disaster" entailed setting up a new hard drive. All of the utilities required are ready to use on the virtual drive.

- Partition the hard drive, using FDISK, to match the size and type as recorded before the disaster:

  ```
  C drive: HPFS primary partition, 200 MB, label "OS2"
  D drive: HPFS logical drive, 1450 MB, label "PROJECT"
  ```

- After partitioning the hard drive, Fdisk requires that the machine be rebooted. Use disk 0 to reboot. Disk 1 and disk 2 will be requested and then the OS/2 prompt appears.
- To format the partitions, use the following commands at the OS/2 prompt:

  ```
  FORMAT C: /FS:HPFS
  FORMAT D: /FS:HPFS
  ```

  Assign to the partitions the same label that was previously used for the drives. ADSM needs the label on the drives to identify the ADSM filespace.
- After this process, the drive is ready to use.

4.3.4 Restore from the ADSM Backup

4.3.4.1 Restoring the Whole System

Now that you have booted the desktop with your OS/2 bootable diskettes, you can invoke the ADSM command line client and take the following steps to restore the entire system:

To restore the whole system from the ADSM backup, invoke the ADSM command line client and issue the following commands:

```
RESTORE C:\* -SUBDIR=YES -REPLACE=YES
RESTORE D:\* -SUBDIR=YES -REPLACE=YES
```

ADSM responds to this command with the following:

```
ADSTAR Distributed Storage Manager
Command Line Backup Client Interface - Version 2, Release 1,Level 0.0
(C) Copyright IBM Corporation, 1990, 1995, All Rigths Reserved.

dsmc> RESTORE C:\* -SUBDIR=YES -REPLACE=YES
RESTORE function invoked.

Please enter password for node "SERVER1": *******

Session established with server ADSM: AIX-RS/6000
  Server Version 2, Release 1, Level 0.2
  Data compression forced on by the server
  Server date/time: 08:30:1996 17:53:11  Last access: 08/30/1996 17:47:55

Restoring            0 C:\TCPCFG.LOG --> C:\TCPCFG.LOG  Done
Restoring          388 C:\AUTOEXEC.01 --> C:\AUTOEXEC.01 . Done
Restoring          368 C:\AUTOEXEC.MGA --> C:\AUTOEXEC.MGA . Done
Restoring        4,278 C:\CONFIG.BK1 --> C:\CONFIG.BK1 . Done
        .        .
        .        .
        .        .
Restore processing finished.
```

4.3.4.2 Restore the ACPs

Boot the OS/2 LAN Server to restart the system. Restore the ACPs for each drive by using the RESTACC utility:

- Issue the RESTACC command to restore the ACPs for the C: drive:

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

  In response, you will get something like this:

```
Restoring Access Control List for C:\.
Restoring Access Control List for C:\HOME\USER02.
Restoring Access Control List for C:\IBMLAN\DCDB.
Restoring Access Control List for C:\IBMLAN\DCDB\APPS.
Restoring Access Control List for C:\IBMLAN\DCDB\DATA.
Restoring Access Control List for C:\IBMLAN\DCDB\DEVICES.
Restoring Access Control List for C:\IBMLAN\DCDB\FILES.
Restoring Access Control List for C:\IBMLAN\DCDB\PRINTERS.
Restoring Access Control List for C:\IBMLAN\DCDB\USERS\USER01.
Restoring Access Control List for C:\IBMLAN\DCDB\USERS\USER01\BATCH.
Restoring Access Control List for C:\IBMLAN\DCDB\USERS\USER02.
Restoring Access Control List for C:\IBMLAN\DCDB\USERS\USER02\BATCH.
Restoring Access Control List for C:\IBMLAN\DCDB\USERS\USERID.
Restoring Access Control List for C:\IBMLAN\DCDB\USERS\USERID\BATCH.
Restoring Access Control List for C:\IBMLAN\DOSLAN\DOS.
Restoring Access Control List for C:\IBMLAN\DOSLAN\NET.
Restoring Access Control List for C:\IBMLAN\NETPROG.
Restoring Access Control List for C:\IBMLAN\REPL\IMPORT\SCRIPTS.
RESTACC completed successfully.
 C:\
```

To restore the ACPs for the D: drive, issue this command:

```
C:\ RESTACC D: /S /V
```

```
Restoring Access Control List for D:\.
Restoring Access Control List for D:\PGM1.
Restoring Access Control List for D:\PGM1\limit1.
RESTACC completed successfully.
 C:\
```

Note: The BACKACC utility we used before the disaster produced a backup copy of NET.ACC and NET.AUD in the NETACC.BKP and NETAUD.BKP files, respectively. You could also manually restore NET.ACC and NET.AUD from these files.

4.3.4.3 Verify the Postdisaster Restoration

An optional step in our recommendations for predisaster preparation was to save some information that would help in the postdisaster recovery verification (see 4.2, “Predisaster Preparation” on page 62). We could then compare the predisaster snapshot with the postdisaster recovery environment to ensure that the restoration was complete.

One of the tools we used to compare pre- and post-disaster tallies (for example, of the CHKDSK command on OS/2) was the

```
DIFF
```

command on AIX (we just used the machine our ADSM server was on).

The DIFF program is used to compare the output of the DIR commands issued after the backup and after the restore. It runs under AIX, so to use it on an AIX workstation you have to:

1. Copy to a diskette the output of the files to be compared.
2. Use the AIX dosread command to copy the files onto an AIX machine.
3. Assuming you are logged on to the AIX machine as the root user, you would use the following commands:

```
cd /home/root

dosread drivec.bef drivec.before
dosread drivec.aft drivec.after
dosread drived.bef drived.before
dosread drived.aft drived.after
```

4. The ″after″ and the ″before″ used in the file names indicate after and before the restore. AIX is case sensitive, so use the file names exactly as typed the first time. Invoke the DIFF program, using the following commands:

```
diff drivec.before drivec.after > diffc.out
diff drived.before drived.after > diffd.out
```

5. Scan the output files using these commands:

```
more diffc.out
more diffd.out
```

6. By inspection, search in the output file to find and justify any differences that exist. For example, in our CHKDSK compare output:
   - The date and time of the directories of course were different before and after the disaster recovery as they had been re-created.
   - The files themselves kept the same date and time. So any file names that appear as output to the DIFF program must be a delta between the pre- and post-disaster recovery environments (or perhaps the number of bytes was changed.)

We also performed some functional tests after the system was rebooted, to verify the restoration. For example:

- As an administration test, try to add and delete a new user to the OS/2 LAN Server.
- As an end-user test, try to send mail to another node server. Verify the mail flow in both directions.

These are only some ideas. Such verification tests are by their very nature installation specific, so you have to think about what is most appropriate for your environment.

Chapter 5. OS/2 Warp Server Recovery from an OS/2 CID Peer Workstation

In this chapter we explain how to recover a OS/2 Warp Server Entry desktop environment by using an OS/2 CID Peer workstation to restore its files through NetBIOS.

We review the kind of information to back up in preparation for a disaster and explain how to use an OS/2 CID Peer workstation and a set of bootable diskettes to recover after a disaster.

You can also use the bootable, direct method to recover if you are not using APPC. Chapter 4, "OS/2 LAN Server: Bootable, Direct Recovery" on page 61 covers the method for OS/2 LAN Server. You may easily adapt the method described there for use with OS/2 Warp Server.

Note: When we finished testing this method, it occurred to us that it would be possible to use a CID Peer Workstation to recover any operating system that used a file system that was usable by the OS/2 peer. Accordingly we include a generic chapter that covers OS/2 V3, OS/2 V4, OS/2 LAN Server, OS/2 Warp Server, DOS/Windows, and Windows 95—see Chapter 6, "Recovery of OS/2 and Windows from an OS/2 CID Peer" on page 107. We still include this chapter to provide a specific, worked example for OS/2 Warp Server.

5.1 Product Overview

OS/2 Warp Server provides a set of selectable services that enable you to customize the server for your specific environment.

5.1.1 OS/2 Warp Server Entry

OS/2 Warp Server Entry provides:

- File and print sharing services. On OS/2 Warp Server these services are based on the IBM LAN Services V5.0, a network operating system for sharing data, aplications, printers, and serial devices across the LAN. For more detail see Chapter 4, "OS/2 LAN Server: Bootable, Direct Recovery" on page 61
- TCP/IP. OS/2 Warp Server provides TCP/IP communications and a set of TCP/IP applications to use the global Internet or create your own intranet.
- Remote access to enable remote systems to dial in and access resources on your LAN.

- System management services based on IBM SystemView for OS/2, an application to manage group or individual systems on your LAN.
- Backup and recovery to save your system against loss of information. Provides integration with ADSM.
- Advanced print based on IBM Print Services Facility for OS/2.

5.1.2 OS/2 Warp Server Advanced

OS/2 Warp Server Advanced enables you to exploit the benefits of using the 386-HPFS: improved performance, directory space management, and local security. It also provides support for symmetric multiprocessing and takes advantage of the fault tolerance provided by the use of disk arrays, mirroring, and duplexed disk volumes.

5.2 Predisaster Preparation

The disaster we are preparing for is the total and catastrophic loss of the ADSM client, where provision has to be made to restore everything from the bare metal up. If our disaster recovery preparations can cover this worst case scenario, we can assume that they will also be able to handle recovery from lesser disasters.

In this section we discuss the information to collect and save before a disaster to enable a bare metal restore.

5.2.1 ADSM Backups

If recovery of the operating system is to be from ADSM, a full backup that includes system files must be taken. This is not the default. The system files will of course be specific to the configuration of the machine being backed up. Figure 20 on page 85 shows the predisaster normal backups being taken.

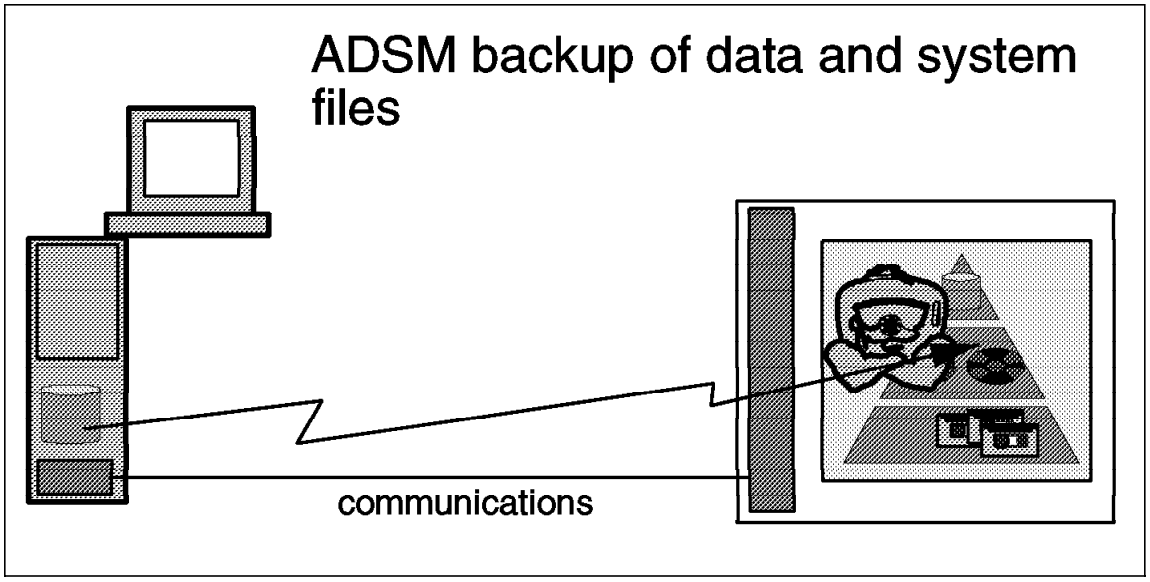


Figure 20. Full ADSM Backup: OS/2 Warp Server

We recommend that you use the following options for the ADSM backup that you will use for the ADSM bare metal restore restore:

- Set the **Copy Serialization** parameter in the **Backup Copy Group** definition to **Shared Static**. This setting allows only those files not being modified to be included in the ADSM backup (preventing a ″fuzzy″ backup). When using this setting, it is best to schedule the ADSM backup during a period of low utilization of the ADSM client. Because this ADSM backup is oriented to provide an image of the workstation to be used in case of disaster, all applications and subsystems running on the machine should be closed before the backup, so that you have the fewest number of open files.
- Because we depend on the existence of an ADSM backup that would provide full restoration of the ADSM client being recovered, we recommend that the ADSM options file, DSM.OPT, only EXCLUDE the SWAPPER.DAT and the EA DATA.SF files. This recommendation implies that you include the operating system software on the C: drive in the ADSM backup. The bootable diskettes will provide only a skeleton version of OS/2 that will enable the ADSM client to function. The assumption is that the newly booted system with the ADSM client will be used to restore the rest of the OS/2 system from an ADSM backup done *for that client.* This may be contrary to your current backup policy (you may currently deliberately EXCLUDE the C: drive from your ADSM backups). This backup should also include empty directories.

- Complete at least one incremental ADSM backup to capture any empty directories. The domain control database (DCDB) may have empty directories if you do not have external serial devices, files, or printer resources. OS/2 LAN Server will attempt to use them at startup and will fail if they are not found.
- Back up the ACPs, which protect access to files and directories. Here is an overview of the steps required to back up the ACPs:

  1. Use the OS/2 LAN Server BACKACC utility to produce a list of the ACPs in a file that ADSM can back up. The BACKACC utility copies the NET.ACC file containing server-unique information, LAN userids, group IDs, passwords, and all of the ACPs (if OS/2 LAN Server Entry) or all of the ACPs except those of the files and directories in the 386-HPFS (if OS/2 LAN Server Advanced). If you are using the OS/2 LAN Server Advanced 386-HPFS, for each drive BACKACC will back up the ACPs for the files and directories in an additional file called ACLBAKx.ACL, where x is the drive letter. In this case, you must use the BACKACC command once for each drive. You may override the file name with the

     `/f:`

     parm.

  2. Run the BACKACC.EXE utility to back up the NET.AUD file containing audit log information for the server. Here is the command you can use to run the BACKACC.EXE utility in a Warp Server Entry environment with HPFS:

     ```
     BACKACC
     ```

     The NET.ACC file will be copied to:

     ```
     C:\IBMLAN\ACCOUNTS\NETACC.BKP
     ```

     And the NET.AUD file will be copied to:

     ```
     C:\IBMLAN\ACCOUNTS\NETAUD.BKP
     ```

     Note: Since we did the tests for this chapter we have found that the NET.AUD file backup, NETAUD.BKP, is stored in the \ibmlan\logs directory instead of \ibmlan\accounts when the NET.AUD file was in the \logs subdir.

     The *access control list* will not be copied because the ACPs for the HPFS and FAT file system are contained in NETACC.BKPP. In this case you need issue the comand only once.

     There is the output from the command:

```
C:\BACKACC

Successfully backed up NET.ACC to NETACC.BKP.
Successfully backed up NET.AUD to NETAUD.BKP.
BACKACC completed successfully.
C:\
```

- OS/2 LAN Server Advanced does not provide a utility to back up the directory size limits. A method for doing so through the LAN Server API is described in *Using ADSM to Back Up OS/2 LAN Server and Warp Server,* SG24-4682.

5.2.2 Operating Environment of the ADSM Client

In preparation for disaster recovery we recommend that you collect and save offsite the information listed below in addition to the ADSM backup data. Depending on your installation, you could save this information by using the DRM feature, or you could save it on hardcopy stored offsite. The way in which you save the information is not as important as ensuring that it is saved somewhere where it can be easily retrieved along with the client recovery media when a disaster occurs.

- **Hardware configuration**

  Keep information about machine type, bus type, hard disk attachment, and of course, the type of network adapter used. Collect any such information that will help you re-create the hardware setup of the ADSM client that has been destroyed in a disaster. If you are using a PS/2, for instance, you may also include information about where to find copies of the associated PS/2 hardware reference diskettes in case you find yourself needing to replace a hard disk.

- **Partitioning drives**

  Record how the hard drives are partitioned and labeled. You can collect this information by using the FDISK command. To do the restore ADSM has to know the hard drive label. We recommend that you define hard drive labels that include the drive letter, to make it easier to determine which ADSM filespace should be restored to which drive at disaster recovery time.

- **Communication details**

  Specific information about your installation communications setup (for example, TCP/IP addresses of the ADSM client and server; SUBNET, ROUTE, and DOMAIN name; TCP/IP port number of the ADSM service; and ADSM node name). This information could be customized on the

bootable diskettes. However, if one set of bootable diskettes will be used to service many OS/2 clients, you may want to store this data for each individual client (using offsite hardcopy or DRM).

Optional: Statistics for Postdisaster Recovery Verification

You may want to gather and save information that can be used after a disaster recovery test once the restore process is completed, to validate that all information has indeed been restored correctly. Each installation will have its own ideas about the best way to verify that the recovery is complete. Some possible sources of information for recovery verification are:

- ADSM statistics at the end of the backup, such as the Number of Objects Inspected, would give a tally of the directories and files on the client being backed up.
- CHKDSK command output for each backed up disk

  Run CHKDSK for each drive being backed up and record:

  – *X* number of kilobytes used in *A* number of directories
  – *Y* number of kilobytes used in *B* number of user files
  – *Z* number of kilobytes used in extended attributes

  For FAT drive records:

  – *X* number of kilobytes used in *A* hidden files
  – *Y* number of kilobytes used in *B* number of directories
  – *Z* number of kilobytes used in *C* user files
- DIR command output

  Collect the output of the DIR /A /S command in a file for each drive. After disaster recovery testing, use the output to compare the files available before the test. Utilities such as the AIX DIFF program could be used for this kind of comparison.
- Other test scripts used during your installation's periodic disaster recovery tests.

5.2.3 Creating the Bootable Diskettes

The technique described here allows you to recover a Warp Server workstation in the event of a disaster.

To recover the damaged workstation, we used a combination of an OS/2 CID Peer workstation and a set of OS/2 bootable diskettes containing:

```
LAN support files
NetBIOS support files
LAN CID Code Server
```

Use the bootable diskettes to run the OS/2 CID Code Server on the damaged Warp Server workstation.

This allows to you access the disks drives of the damaged Warp Server workstation from another OS/2 CID Peer machine.

The assisting OS/2 CID Peer workstation had installed:

```
LAN Support files to use NetBIOS communication protocol
LAN CID Client Redirector files
ADSM Client code
```

The OS/2 CID Peer machine works as a **CID Client Redirector** and uses the disk drives on the damaged Warp Server workstation over the LAN through NetBIOS. The Warp Server workstation is recovered by using ADSM client code running on the OS/2 CID Peer workstation.

The method described here facilitates recovery of the damaged Warp Server without dependence on the communication method used on the damaged workstation to communicate with the ADSM server. See Figure 21 on page 90.

Therefore you can recover a machine that uses a communication method that is not possible to run from bootable diskettes (for example, APPC), provided an OS/2 CID Peer machine can contact the ADSM server using any communication protocol and access the drives on the damaged machine using the CID redirection code.

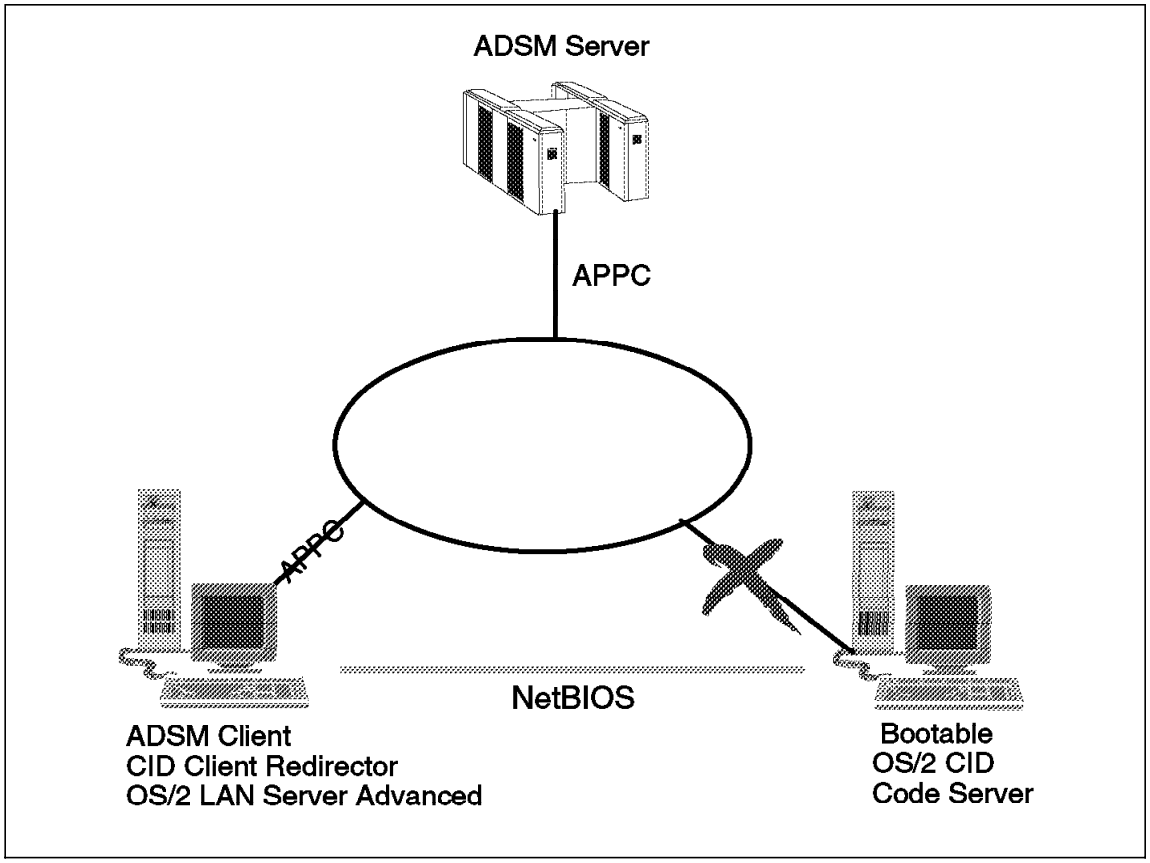


Figure 21. Scenario for Peer Recovery Using CID

Where to find more information about CID

OS/2 Installation Techniques: The CID Guide (GG24-4295-00) is the basic reference guide for CID management of software in a LAN environment.

5.2.3.1 Configuration Used to Test the Technique

- Our peer recovery machine ran OS/2 Warp using a token-ring adapter and was configured to use NetBIOS.
- The damaged machine to be recovered used a token-ring adapter card and a file system compatible with the OS/2 CID Peer recovery machine.
- Any ADSM server using a communication method supported by the OS/2 CID Peer workstation can be used.
- Personal Computer 750
- 16 Mbps token-ring attachment

- 1.6 GB IDE-attached hard drive, partitioned as follows:
  - C drive: HPFS primary partition, 200 MB, label ″OS2″
  - D drive: HPFS logical drive, 1450 MB, label ″PROJECT″
- IBM OS/2 Warp Server with WinOS/2 Version 4.00
- OS/2 LAN Server Version 5.0
- ADSM/2 Version 2, Release 1, Level 0.3 client code
- HPFS
- AIX Version 2, Release 1, Level 0.2 server code

To use this technique you will need:

- Three formatted 1.44 MB diskettes
- OS/2 Warp system installation diskettes
- The MPTS disk 5 from the Warp Server installation diskettes, or the Warp Server installation CD-ROM.

5.2.3.2 Step-by-Step Instructions

These instructions to create a set of OS/2 Warp, NetBIOS, and CID Code Server enabled bootable diskettes are based on the method provided by Kenneth Morse of the IBM Washington Systems Center. The diskettes are created to use HPFS but include the references to 386-HPFS system for your information.

Step 1: Create the Base OS/2 Diskettes: Format three 1.44 MB diskettes and label them disk 0, disk 1, and disk 2. Make a diskCOPY of the OS/2 Warp startup diskette disk 0 to the new disk 0, and diskCOPY the OS/2 Warp installation diskette disk 1 to the new disk 1. Disk 0 is ready to use without change, disk 1 needs some files to be deleted to make space for following steps. Disk 2 will be created later.

Please note that we used the Startup diskette disk 0, and the Installation diskette disk 1 of the OS/2 Warp operating system to obtain the base bootable diskettes. See Appendix A, “Alternative Methods to Create Base OS/2 Bootable Diskettes” on page 269 for more information about using alternatives.

Step 2: Edit the Base OS/2 Diskettes by Deleting Files: Remove the following files from disk 1 if it was created from a diskCOPY of installation diskette 1:

```
OS2LOGO.
BUNDLE.
FDISK.COM
SYSINST2.EXE
XDFLOPPY.FLT
DEL.LST
MOUSE.SYS
SIPANEL1.DLL
SYSLEVEL.OS2
```

Step 3: Edit the Base OS/2 Diskettes to Add Files: Once you create the base OS/2 diskettes, add the following files:

- **OS/2 files**

  Below is a list of OS/2 files that you must copy to or create and then copy to disk 1.

```
File Name     Found in
---------------------------------------
VDISK.SYS   - \OS2 -or - \OS2\BOOT
NLS.DLL     - \OS2\DLL
STARTUP.CMD - See B.1, "STARTUP.CMD" on page 271.
FINDRAM.CMD - See B.2, "FINDRAM.CMD" on page 271.
THE.CMD     - See B.3, "THE.CMD" on page 272.
PART2.CMD   - See B.4, "PART2.CMD" on page 273.
PART3.CMD   - See B.5, "PART3.CMD" on page 274.
SETUP.CMD   - See B.7, "SETUP.CMD" on page 276.
An editor   - To dynamically choose your settings at
              boot time, you must have a copy of a tiny
              editor (for example, TEDIT, which comes with
              OS/2 Warp).  Any editor will do as long as it
              does not need a graphical interface and fits
              on the 1.44 MB diskette.
```

- **LAN support files**

  You must have the support layer necessary to operate your network card at the hardware level. Below is a list of files that you have to add to disk 1. Next to each file name is a hint as to where to find it on a working LAN-attached system.

```
File Name     Found in
---------------------------------------
LANMSGEX.EXE - \IBMCOM
PROTOCOL.INI - \IBMCOM
LANMSGDD.OS2 - \IBMCOM
PROTMAN.OS2  - \IBMCOM
LTO.MSG      - \IBMCOM
LT2.MSG      - \IBMCOM
```

```
PRO.MSG      - \IBMCOM
LANMSGDL.DLL - \IBMCOM\DLL
IBMTOK.OS2   - \IBMCOM\MACS
NETBIND.EXE  - \IBMCOM\PROTOCOL
```

- **NetBIOS files**

  For NetBIOS support, the following files must be copied from a working NetBIOS system to disk 1:

```
Filename      Found in
----------------------
NETBEUI.OS2   \IBMCOM\PROTOCOL
NETBIOS.OS2   \IBMCOM\PROTOCOL
```

- **386-HPFS files**

  Optionally, if you are using Warp Server Advanced with 386-HPFS, add the following files to disk 1 to include 386-HPFS support:

```
Filename      Found in
----------------------
386-HPFS.IFS  -IBM386FS
386-HPFS.INI  -IBM386FS
HFS.MSG       -IBM386FS
BOOTSH.EXE    -IBM386FS
BSH.MSG       -IBM386FS
BSHH.MSG      -IBM386FS
```

Step 4: Modify CONFIG.SYS and CMD Files: Make the following modifications to the CONFIG.SYS file on disk 1:

- **References in CONFIG.SYS**

  Remove any reference on the CONFIG.SYS to the following files:

```
XDFLOPPY.FLT
MOUSE.SYS
```

- **Change path statements**

  Change the three path statements so that they reference the A: drive:

```
LIBPATH=.;\;A:\;
SET PATH=.;\;A:\;
SET DPATH=.;\;A:\;
```

- **Modify initialization parameters**

  To correctly execute the STARTUP.CMD, include the following lines in your CONFIG.SYS:

```
PROTSHELL=SYSINST1.EXE
SET OS2_SHELL=CMD.EXE /K STARTUP.CMD
```

Note on 386-HPFS

To correctly install the 386-HPFS and execute the STARTUP.CMD, include the following lines in your CONFIG.SYS file instead:

```
PROTSHELL=BOOTSH.EXE CMD.EXE /K STARTUP.CMD
IFS=386-HPFS.IFS A:\386-HPFS.INI /AUTOCHECK:
SET OS2_SHELL=CMD.EXE
```

- **Device drivers**

  All device drivers copied to disk 1 must be referenced at startup time. Add the following lines to the bottom of CONFIG.SYS (naturally, include the NetBIOS driver only if you plan to use NetBIOS instead of TCP/IP):

```
REM *** Protocol/LAN/VDISK Drivers ***
DEVICE=\VDISK.SYS 4069,,
DEVICE=\LANMSGDD.OS2 /I&colonA:\
RUN=\LANMSGEX.EXE
DEVICE=\PROTMAN.OS2 /I&colonA:\

REM *** Appropriate Network Adapter Driver Here ***
DEVICE=\IBMTOK.OS2

REM *** NETBIOS DRIVERS ***
DEVICE=NETBEUI.OS2
DEVICE=NETBIOS.OS2

REM *** Netbind ***
RUN=\NETBIND.EXE
```

Step 5: Create Disk 2: To create disk 2 you will need a pair of compression-decompression utilities. Disk 2 will contain compressed versions of the NetBIOS files, OS/2 utilities, CID Code Server files, and an appropriate decompression utility. Here are the steps to create disk 2:

- **Create a temporary directory**

  To collect all necessary files, create a new directory called something like C:\TEMPADSM. Switch to C:\ and issue:

```
MD TEMPADSM
```

- **NetBIOS files**

  Copy this file to the temporary directory \TEMPADSM:

```
ACSNETB.DLL
```

- **Utilities**

  The following utilities are not required to successfully run the CID code server, but they can come in quite handy, so copy them to \TEMPADSM:

```
FDISK.COM    - For repartitioning if necessary
FORMAT.COM   - For reformatting if necessary
LABEL.COM    - For changing volume names
CHKDSK.COM   - For repairing filesystem damage
UHPFS.DLL    - Required for HPFS partition work
ATTRIB.EXE   - For altering file attributes
MAKEINI.EXE  - For repairing/rebuilding the OS/2 INI file
XCOPY.EXE    - For copying files
INI.RC       - Seed file for MAKEINI
INISYS.RC    - Seed file for MAKEINI
LOCK.RC      - Seed file for MAKEINI
SYSINSTX.COM - For bootstrap sector initialization
TEDIT.EXE    - An text editor
OSO001.MSG   - OS/2 Message repository
```

OS0001.MSG

Because of space restrictions, we did not put this file on disk 1. This is the stock OS/2 message file. When you finally use the diskettes to boot OS/2 LAN Services, you will get a message stating that the operating system could not find message 1467. If you were to type HELP SYS1467 on a different machine, you would see:

```
SYS1467:  VDISK Version 2.1 Virtual disk ***
disk Size:           *** KB
Sector Size:         ***
Directory Entries:   ***
```

In other words, don't worry about it!

Feel free to include any other little utilities you think may come in handy when working on a damaged system; your only limit is the amount of space that can be compressed to fit on a 1.44 MB diskette.

- **CID Code Server files**

  To run the CID Code Server, include the CID Code Server files as follows:

Extracting the LAN CID Utilities Files

Extract the CID Code Server files from the LAN CID Utilities (LCU) included with OS/2 Warp Server on MPTS diskette 5 or in the Warp Server CD-ROM. Use the following sample:

Create a temporary directory:

```
CD C:
MD TMPLCU
```

Change to the directory you have created

```
CD TMPLCU
```

To extract the files from MPTS diskette 5 in your A: drive to temporary directory C:\TMPLCU, execute the following commands:

```
PKUNZIP2 A:\SRVIFS\SRVIFS.ZIP
    COPY A:\README.UTL
```

To extract the files from the Warp Server CD-ROM in your X: drive to temporary directory C:\TMPLCU, execute the following commands:

```
PKUNZIP2 X:\CID\SERVER\IBMLS\IBM5OON5\SRVIFS.ZIP
    COPY X:\CID\SERVER\IBMLS\IBM5OON5\README.UTL
```

Now the required files are available on your TMPLCU directory.

Read the README.UTL file, which includes technical information about MPTS.

Copy the following files to the C:\TEMPADSM directory:

Filename	Found in
SERVICE.EXE	-TMPLCU
XI1.MSG	-TMPLCU
XI1H.MSG	-TMPLCU
RESCUE1.INI	-See B.8, "RESCUE1.INI" on page 277.

(The RESCUE.INI contains the initialization parameters for SERVICE.EXE.)

- **Build the zip file**

  If you use the PkZip2 and PKUnZip2 utilities with C:\TEMPADSM as the temporary directory, execute the following commands to build the zip file on disk 2:

```
C:
CD C:\TEMPADSM
PKZIP2 ADSMPACK.ZIP *
```

If you are using the ZIP and UNZIP utilities, execute the following commands to compress all of the files you gathered together into a file named ADSMPACK.ZIP:

```
C:
CD C:\TEMPADSM
ZIP ADSMPACK.ZIP *
```

Copy this file to disk 2.

- **Copy the decompression utility**

  Copy the corresponding decompression program (PKUNZIP2.EXE or UNZIP.EXE) to disk 2. If you use InfoZip′s UNZIP.EXE, you will have to copy the NLS.DLL file from your \OS2\DLL subdirectory onto disk 2.

Make sure you edit PART2.CMD on disk 1 and specify which decompression utility you will be using!

5.2.4 Setting Up the OS/2 CID Peer Workstation

This recovery method uses an OS/2 CID Peer workstation to restore drives of the failed Warp Server machine.

The OS/2 CID Peer workstation that you use must be able to use the NetBIOS communication protocol to allow the CID Client Redirection program SRVATTCH.EXE to succesfully attach the disks drives of the failing Warp Server machine. Also the workstation must be able to manage the file system used on the failing system.

The failing Warp Server machine will be running CID CODE Server program SERVICE.EXE from the bootable diskettes that you have prepared.

5.2.4.1 Step-by-Step Instructions

This very simple process has only two steps, as described below:

Step 1: Install the CID Client Redirection Files: The files are available on the TMPLCU directory that you created when you built the bootable diskettes. Copy the following files from the TMPLCU directory to the root directory of the C drive on the OS/2 CID Peer workstation:

```
Filename      Found in
----------------------
SRVIFS.SYS   -TMPLCU
SRVIFSC.IFS  -TMPLCU
SRVATTCH.EXE -TMPLCU
XI1.MSG      -TMPLCU
XI1H.MSG     -TMPLCU
```

For simplicity we used the root directory on the C: drive, but you can use any convenient directory. Remember to change your CONFIG.SYS file accordingly.

Step 2: Edit the CONFIG.SYS File: First, back up your CONFIG.SYS file. Then use an editor to add the following lines to the end of your CONFIG.SYS:

```
REM --- CID Client Redirection  ---
DEVICE=C:\SRVIFS.SYS
IFS=C:\SRVIFSC.IFS SERVER1
```

Reboot your OS/2 CID Peer workstation to activate the statements.

5.3 Postdisaster Recovery

In this section we describe how to recover from a disaster to the OS/2 LAN Server Advanced Version 4 ADSM client using the information we saved before the disaster (described in 5.2, “Predisaster Preparation” on page 84) and the bootable diskettes we created (described in 5.2.3, “Creating the Bootable Diskettes” on page 88).

To simulate a disaster, we reformatted the C: and D: drives so that the machine would no longer boot.

Having done this, after a disaster to the ADSM client we are positioned to begin the bare metal restore. We summarize the steps taken below.

5.3.1 Rebuild Hardware Environment

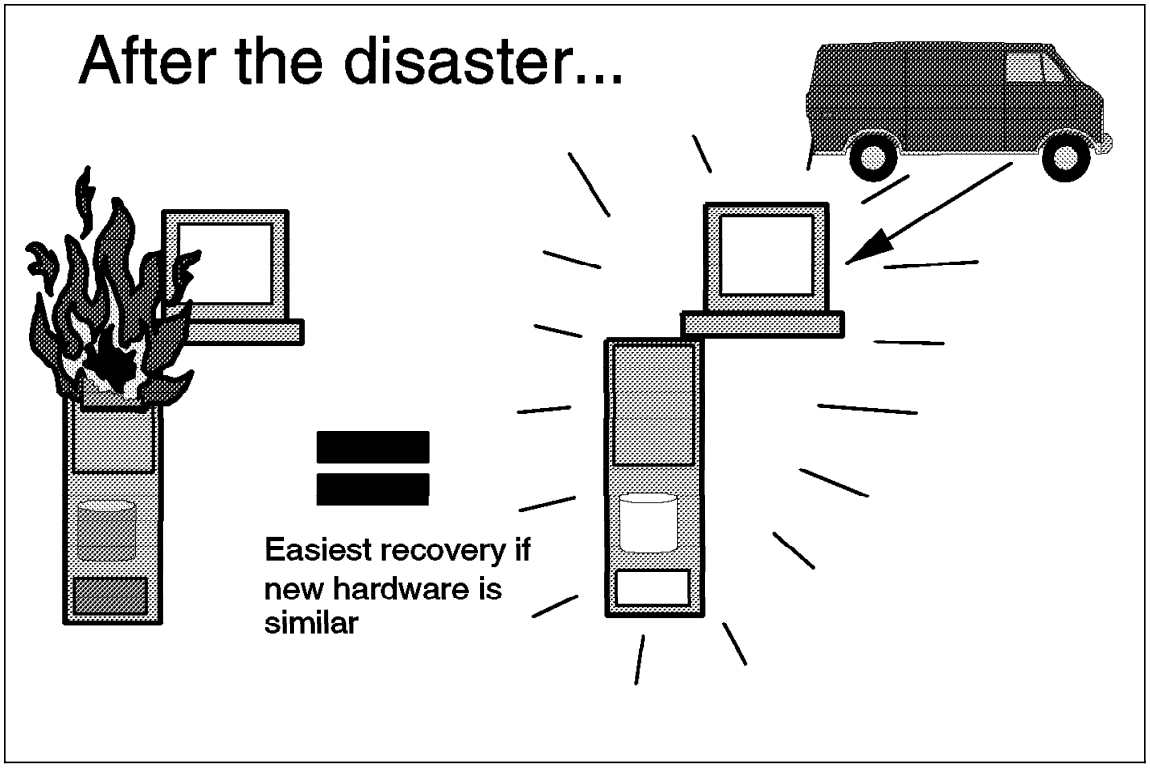


Figure 22. Recreating the OS/2 Warp Server Hardware Environment

Retrieve information about the OS/2 machine to help re-create the hardware environment of the destroyed ADSM client. The new replacement machine must have a similar configuration.

If DRM had been used as the repository for this type of information, you could retrieve it by issuing the appropriate ADSM queries to the ADSM server. For examples of these queries, see 1.3.6, “Disaster Recovery Manager” on page 18.

5.3.2 Boot the Recovery System

Use the Warp Server recovery bootable diskettes to boot the replacement hardware and prepare the workstation to run the OS/2 CID Code Server. Follow these steps:

- Boot the machine with disk 0, until the blue screen asking for disk 1 appears.
- Insert disk 1 and press <ENTER>. At this point you see messages that indicate a succesful LAN and NetBIOS startup:

```
SYS0318: Message file OSO001.MSG cannot be found for message  1467.

IBM OS/2 LANMSGDD ( 04/26/95 ) 2.01 is loaded and operational.
IBM OS/2 LAN Protocol Manager

IBM OS/2 NETBEUI 5.00.0
NETBEUI: Using a 32-bit data segment
IBM OS/2 NETBIOS 4.0
Adapter 0 has 254 NCBs, 254 sessions, and 41 names available to NETBIOS
applications
NETBIOS 4.0 is loaded and operational.
```

Message SYS0318

The SYS0318 message reports that a repository file is not available to retrieve the contents of message 1467. The format of message 1467 is:

```
SYS1467: VDISK Version 2.1 Virtual disk ***
disk Size:          4000 KB
Sector Size:        512
Directory Entries:  64
```

After a few moments the screen clears and you see:

```
ADSM BOOTABLE RECOVERY STARTED.........
*****************************************
 .
Searching for a VDISK
VDISK Found as drive (E:\)
 .
Copying files to drive (E:\)
 .
Unpacking file to VDISK
Wait for all diskette activity to stop, (background processes..)
Remove diskette 1 from the drive, and insert diskette 2 and then
Press any key when ready  . . .
```

- Wait for all activity to stop, remove disk 1, insert disk 2, and press <ENTER>. Wait for the message requesting disk 1 again:

```
Working...
PKUNZIP (R) FAST!  Extract Utility  Ver. 1.09-OS/2 Prot Mode 1-15-91
Copr. 1989-1991 PKWARE Inc. All Rigths Reserved PKUNZIP/h for help
PKUNZIP Reg. U>S> Pat. an Tm. Off.     IBM LICENSED VERSION


Searching ZIP: A:ADSMPACK.ZIP
  Exploding: acsnetb.dll
  Exploding: ATTRIB.EXE
  .
  .
  .
  Exploding: XI1.MSG
  Exploding: XI1H.MSG
Done...
Please remove diskette 2 from the drive, and insert diskette 1 and then
Press any key when ready  . . .
```

- After removing disk 2, inserting disk 1, and pressing <ENTER>, the tiny editor TEDIT.EXE shows the contents of RESCUE1.INI, which contains the initialization parameters for the SERVICE.EXE program.
- You must define as many ALIAS lines as the drives you will be restoring. Also the drive referenced on an ALIAS sentence must exist, or you will get an error.

  Here is a sample of the screen that you see:

```
==== Top of File ====
*
* RESCUE1.INI file  used by SERVICE.EXE
* ------------------------------------
* Edit the values or add more ALIAS sentences if required.
* Then, save to continue.
*
Name=RESCUE1
GroupName=yes
Adapter=0
MaxClients=1
Path=C:\
PermitWrite=no
MaxFiles=100
ClientWorkers=6
Alias=readwrite,single,diskC,C:\
Alias=readwrite,single,diskD,D:\
==== End of File ====


c:\tempadsm\rescue1.ini                                        1     1
F1=Help F2=Save F3=Quit F4=File F5=Cmd F7=Name F8=Edit F9=Undo F10=Next
```

We saved this information when creating RESCUE1.INI on the original OS/2 bootable disk 1, so we did not have to do any editing. If you do have to make changes to RESCUE1.INI, you can save the changes by pressing F4.

- After the Initialization Complete messages, the OS/2 prompt appears. At this point you can start the CID Code Server. Alternativey, you may have to perform some preliminary tasks using the OS/2 utilities, for example, repartitioning a new hard drive using the FDISK utility.

```
Initialization Complete
 .
To Start the CODE Server, enter:
 .
SERVICE /INI=RESCUE1

E:\
```

5.3.3 Set Up a New Hard Drive

The nature of our ″disaster″ entailed setting up a new hard drive. All of the utilities required are ready to use on the virtual drive.

- Partition the hard drive, using FDISK, to match the size and type as recorded before the disaster:

  ```
  C drive: HPFS primary partition, 200 MB, label ″OS2″
  D drive: HPFS logical drive, 1450 MB, label ″PROJECT″
  ```

- After partitioning the hard drive, FDISK requires that the machine be rebooted. Use disk 0 to reboot. Disk 1 and disk 2 will be requested, and then the OS/2 prompt appears.

- To format the partitions, use the following commands at the OS/2 prompt:

  ```
  FORMAT C: /FS:HPFS
  FORMAT D: /FS:HPFS
  ```

  Assign to the partitions the same label that was previously used for the drives. ADSM needs the label on the drives to identify the ADSM filespace.

- After this process, the drive is ready to use.

5.3.4 Restore from the ADSM Backup

5.3.4.1 Restoring the Whole System

To restore the whole system from the ADSM backup, do the following:

- To activate the CID Code Server on the machine to be recovered (on the damaged Warp Server workstation), issue the following command:

  ```
  SERVICE /INI=RESCUE1
  ```

  The CID Code Server will be activated and you will see the following screen:

  ```
  E:\service /ini=rescue1
  RESCUE1 Server is active, Version 1.32.2
  ```

  At this point, the CID Code Server is active on the machine to be recovered. All other activities to complete the restoration have to be performed on the OS/2 CID Peer workstation.

  The OS/2 CID Peer recovery workstation is ready to use the disk drives on the failing Warp Server machine. All that you have to do is issue the SRVATTCH command to attach the drives through the LAN, using the NetBIOS facilities.

- Open an OS/2 window and issue the following commands:

  ```
  SRVATTCH X: \\RESCUE1\DISKC
  SRVATTCH Y: \\RESCUE1\DISKD
  ```

  where RESCUE1 is the name of the CID Code Server, and DISKC and DISKD are the aliases defined in the RESCUE1.INI file.

  New disks available

  After the commands complete successfully, two new disks are available on your Peer Assistance workstation:

  - The new X: drive is the C: drive on the Warp Server machine.
  - The new Y: drive is the D: drive on the Warp Server machine.

  To verify that you are accessing the drives, issue a DIR command against the new X and Y drives.

- On the OS/2 CID Peer workstation, open an OS/2 window and start the ADSM client program using the same ADSM nodename as the nodename of the failing Warp Server workstation. In our case we issued the following command:

  ```
  DSMC -NODENAME=CANDEMAS
  ```

  where CANDEMAS is the ADSM nodename of the failing Warp server machine.

Be careful and make sure you are connecting to the ADSM server, using the nodename of the failing Warp Server workstation.

At this point, you are connected to the ADSM server and ready to restore.

- At the ADSM prompt, issue the following command:

  ```
  RESTORE -SUBDIR=YES -REPLACE=ALL {OS2}\* X:\
  ```

  We used the filespace name in the restore command because it is independent of the drive label on the OS/2 CID Peer workstation. ADSM responds to the commands with the following:

```
C:\ dsmc -nodename=candemas
ADSTAR Distributed Storage Manager
Command Line Backup Client Interface - Version 2, Release 1, Level 0.0
(C) Copyright IBM Corporation, 1990, 1995, All Rights Reserved.

dsmc> restore -subdir=yes -replace=yes {OS2}\* x:\
Restore function invoked.

Please enter password for node "CANDEMAS": ********

Session established with server ADSM: AIX-RS/6000
  Server Version 2, Release 1, Level 0.9
  Server date/time: 09/18/1996 11:13:01   Last access: 09/18/1996 11:00:4

ANS4166I ***** Examined 1000 files *****
ANS4166I ***** Examined 2000 files *****
Restored directory X:\ADSM\
Restored directory X:\ADSM\API\
Restored directory X:\BOOKS\
Restored directory X:\Desktop\
Restored directory X:\Desktop\ADSM Client\
Restored directory X:\Desktop\IBM Internet[Connection for OS!2\
      .                                    .
      .                                    .
      .                                    .
Restoring      522,877 C:\tcpip\umail\viewcli.dll --> X:\tcpip\umail\view
cli.dll ..... Done
Restoring        1,957 C:\IBMLAN\NETPROG\RDRHELP.200 --> X:\IBMLAN\NETPRO
OG\RDRHELP.200 . Done
Restoring        1,536 C:\IBMLAN\NETSRC\OS2\LIB\UPM32.LIB --> X:\IBMLAN\N
ETSRC\OS2\LIB\UPM32.LIB . Done

Restore processing finished.
dsmc>
```

Repeat the procedure for the Y: drive. Issue this command:

```
RESTORE -SUBDIR=YES -REPLACE=YES {PROJECT}\* Y:\
```

After you complete the restore, reboot the Warp Server. All of your data will be there.

5.3.4.2 Restore the ACPs

We recommended that in preparation for disaster recovery you regularly back up the ACPs using the BACKACC utility. Only restore ACPs after a disaster if you have any problems after the restore, because all of your ACPs are in the NET.ACC file, which is restored by ADSM (remember in this scenario we are working with a Warp Server entry).

5.3.4.3 Verify the Postdisaster Restoration

An optional step in our recommendations for predisaster preparation was to save some information that would help in the postdisaster recovery verification (see 4.2, “Predisaster Preparation” on page 62). We could then compare the predisaster snapshot with the postdisaster recovery environment to ensure that the restoration was complete.

One of the tools we used to compare pre- and post-disaster tallies (for example, of the CHKDSK command on OS/2) was the **DIFF** command on AIX (we just used the machine our ADSM server was on).

The DIFF program is used to compare the output of the DIR commands issued after the backup and after the restore. It runs under AIX, so to use it on an AIX workstation you have to:

1. Copy to a diskette the output of the files to be compared.
2. Use the AIX dosread command to copy the files onto an AIX machine.
3. Assuming you are logged on to the AIX machine as the root user, you would use the following commands:

```
cd /home/root

dosread drivec.bef drivec.before
dosread drivec.aft drivec.after
dosread drived.bef drived.before
dosread drived.aft drived.after
```

4. The ″after″ and the ″before″ used in the file names indicate after and before the restore. AIX is case sensitive, so use the file names exactly as typed the first time. Invoke the DIFF program, using the following commands:

```
diff drivec.before drivec.after > diffc.out
diff drived.before drived.after > diffd.out
```

5. Scan the output files using these commands:

```
more diffc.out
more diffd.out
```

6. By inspection, search in the output file to find and justify any differences that exist. For example, in our CHKDSK compare output:
    - The date and time of the directories of course were different before and after the disaster recovery as they had been re-created.
    - The files themselves kept the same date and time. So any file names that appear as output to the DIFF program must be a delta between the pre- and post-disaster recovery environments (or perhaps the number of bytes was changed.)

We also performed some functional tests after the system was rebooted, to verify the restoration. For example:

- As an administration test, try to add and delete a new user to the OS/2 LAN Server.
- As an end-user test, try to send mail to another node server. Verify the mail flow in both directions.

These are only some ideas. Such verification tests are by their very nature installation specific, so you have to think about what is most appropriate for your environment.

Chapter 6. Recovery of OS/2 and Windows from an OS/2 CID Peer

In this section we describe how to use OS/2 CID client redirection and ADSM to recover a damaged workstation in the event of a disaster. The method described can be used to recover the following workstation environments:

- OS/2 V3
- OS/2 V4
- OS/2 LAN Server
- OS/2 Warp Server
- DOS/Windows
- Windows 95 (but see Chapter 8, “Windows 95 Recovery” on page 137 for long file name considerations)

Note: When we finished testing this method as shown in Chapter 5, “OS/2 Warp Server Recovery from an OS/2 CID Peer Workstation” on page 83, it occurred to us that it would be possible to use a CID Peer Workstation to recover any operating system that used a file system that was usable by the OS/2 peer. Accordingly we include this generic chapter that covers OS/2 V3, OS/2 V4, OS/2 LAN Server, OS/2 Warp Server, DOS/Windows, and Windows 95. Refer to the operating-system-specific chapters for details of other backup considerations, for example, type of ADSM backup and use of DRM.

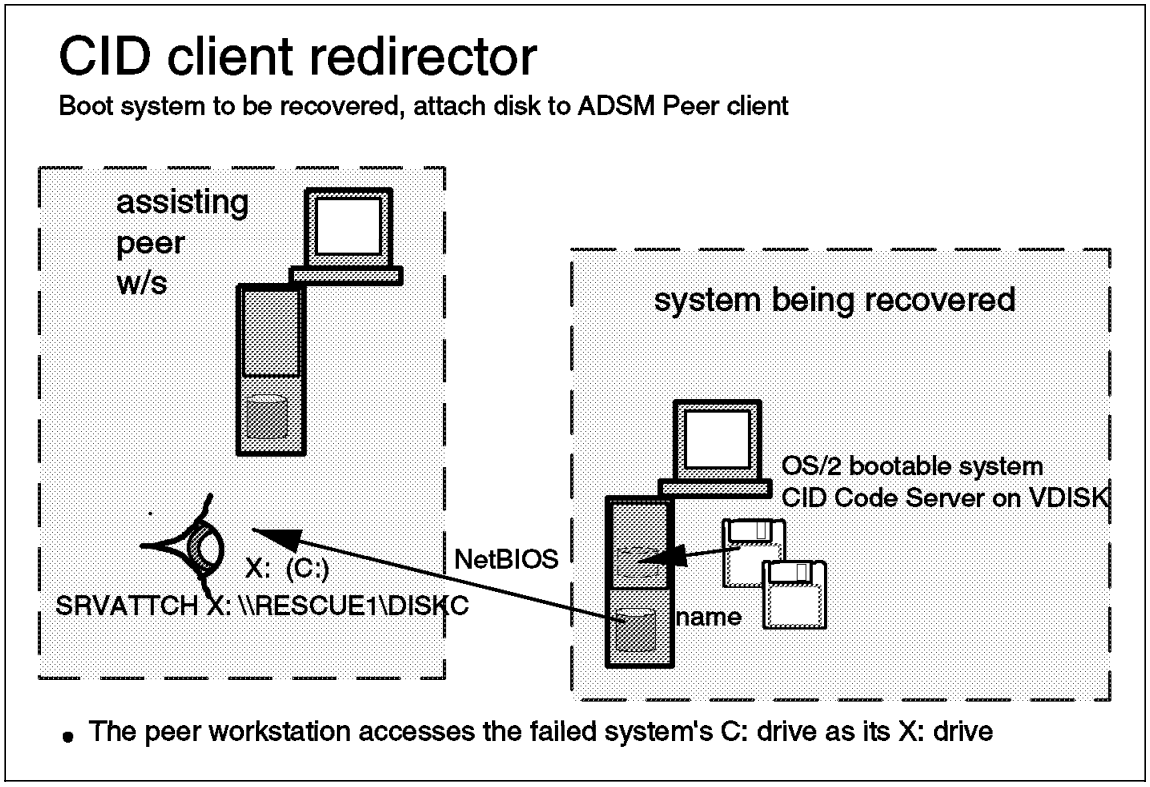


Figure 23. CID Client Redirector. The replacement machine is booted from diskettes. The diskette system has a CID Code Server that is loaded onto a virtual disk. The assisting peer machine then attaches the failed machine's disk(s), using NetBIOS.

You can recover a machine that normally uses an ADSM communication method such as APPC. Another CID Peer machine must be available to retrieve the failed machine's backup data from the ADSM server, and it must be able to access the drives on the damaged one, using the CID redirection code. The OS/2 peer must also be able to use the file system of the failed machine (for example, FAT or HPFS, but not the Windows NT File System (NTFS) or NetWare).

Clearly, if a system image is being restored to replacement hardware, that hardware must be compatible with the image being restored—for example, the disks, disk controllers, and LAN adapter card must be similar to those of the failed machine.

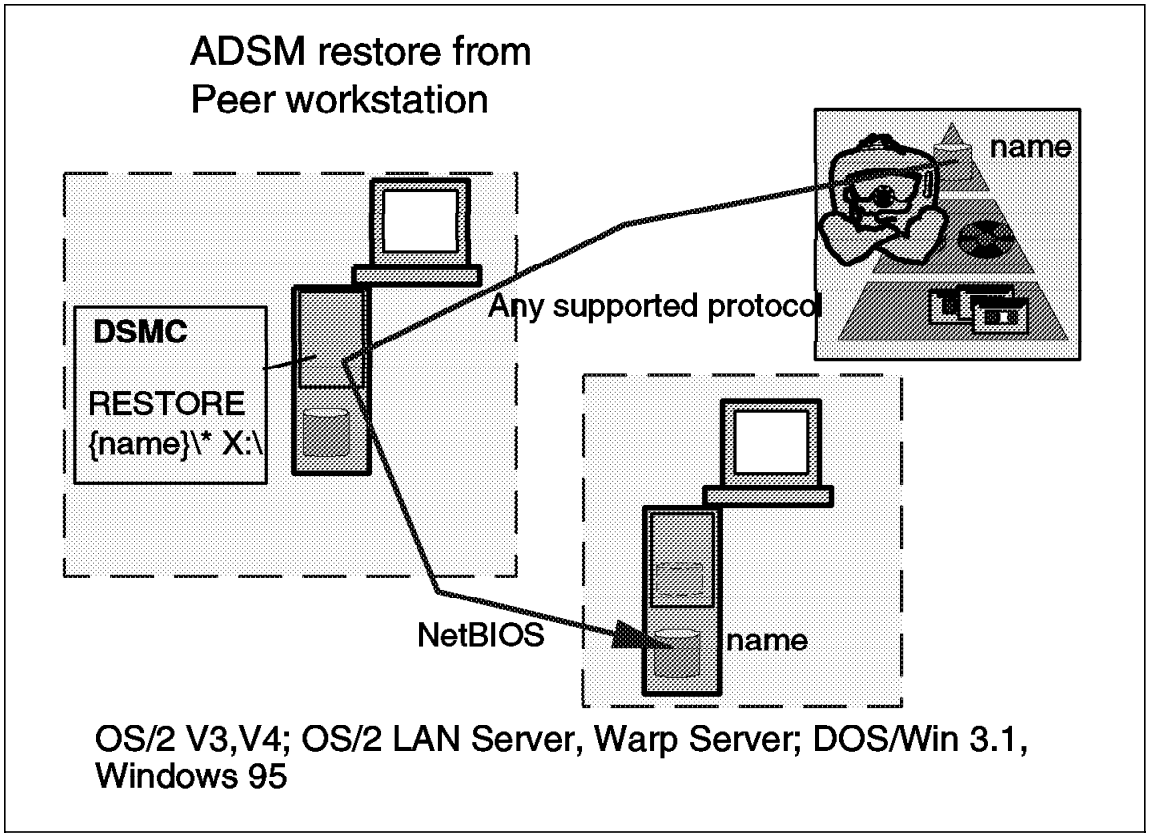


Figure 24. Client Restore from CID Peer over NetBIOS. When the assisting peer machine can see the failing machine's disk(s), an ADSM client is used to restore from the failed machine's backup image from the ADSM server. Once the restore is complete, the failed machine can be rebooted. Because the recovery is done with NetBIOS between the two machines, it is possible to recover a workstation that is normally connected through APPC to the ADSM server.

6.1 Creating the Bootable Diskettes

To recover the damaged machine, we used a combination of an OS/2 CID Peer workstation and a set of OS/2 bootable diskettes containing:

- LAN Support files
- NetBIOS Support files
- LAN CID Code Server

Use the bootable diskettes to run the OS/2 CID Code Server on the damaged workstation so that you can access the drives of the damaged workstation from the assisting OS/2 CID Peer machine.

The OS/2 CID Peer workstation had installed:

- LAN Support files to use NetBIOS
- LAN CID Client Redirector files
- ADSM Client code

The OS/2 CID Peer machine works as an **OS/2 CID Client Redirector** and uses the disks drives on the damaged workstation over the LAN through NetBIOS. The damaged machine is recovered by using the ADSM client code running the OS/2 CID Peer machine.

Where to find more information about CID

OS/2 Installation Techniques: The CID Guide (GG24-4295-00) is the basic reference guide for CID management of software in a LAN environment.

6.1.1 Configurations Used to Test the Technique

- Our peer recovery machine ran OS/2 Warp Version 3 using a token-ring adapter and was configured to use NetBIOS.
- The damaged machine to be recovered used a token-ring adapter card and a file system compatible with the OS/2 CID Peer recovery machine.
- Any ADSM server using a communication method supported by the OS/2 CID Peer workstation can be used.

To use this technique you will need:

- OS/2 Warp system installation diskettes
- The MPTS package (diskette or CD-ROM) shipped with OS/2 Warp Connect, OS/2 LAN Server, or OS/2 Warp Server or included with TCP/IP for OS/2 V2 or OS/2 V3.
- Three formatted 1.44 MB diskettes

6.1.2 Step-by-Step Instructions

These instructions to create a set of OS/2 Warp, NetBIOS, and CID Code Server enabled bootable diskettes are based on the method documented by Ken Morse of the IBM Washington Systems Center. The diskettes are created to use HPFS, but include references to 386-HPFS for your information.

Step 1: Create the Base OS/2 Diskettes: Format three 1.44 MB diskettes and label them disk 0, disk 1, and disk 2. DISKCOPY the OS/2 Warp startup diskette disk 0 to the new disk 0, and DISKCOPY the OS/2 Warp installation diskette disk 1 to the new disk 1. Disk 0 is ready to use without change, and

disk 1 needs some files to be deleted to make space for following steps. disk 2 will be created later.

Please note that we used Startup diskette disk 0 and Installation diskette disk 1 of the OS/2 Warp operating system to obtain the base bootable diskettes. See Appendix A, “Alternative Methods to Create Base OS/2 Bootable Diskettes” on page 269 for more information about using alternatives.

Step 2: Edit the Base OS/2 Diskettes by Deleting Files: Remove the following files from disk 1:

```
OS2LOGO.
BUNDLE.
FDISK.COM
SYSINST2.EXE
XDFLOPPY.FLT
DEL.LST
MOUSE.SYS
SIPANEL1.DLL
SYSLEVEL.OS2
```

Step 3: Edit the Base OS/2 Diskettes to Add Files: Below is the list of OS/2 files you must copy to or create on disk 1. Generally, all of the required files can be found in a working LAN Server or Warp Server workstation.

- **OS/2 files**

  Next to each file name are pointers to where the file should be found. You will find samples for the CMD files in Appendix B, “Contents of Files Added to Bootable Diskettes” on page 271.

Filename	Found in
VDISK.SYS	\OS2\BOOT
NLS.DLL	\OS2\DLL
STARTUP.CMD	See B.1, “STARTUP.CMD” on page 271.
FINDRAM.CMD	See B.2, “FINDRAM.CMD” on page 271.
THE.CMD	See B.3, “THE.CMD” on page 272.
PART2.CMD	See B.4, “PART2.CMD” on page 273.
PART3A.CMD	See B.6, “PART3A.CMD” on page 275.

- **LAN support files**

  You must have the support layer necessary to operate your network card at the hardware level. Copy the following files to disk 1 from a working LAN-attached system:

```
Filename      Found in
----------------------
LANMSGEX.EXE  \IBMCOM
PROTOCOL.INI  \IBMCOM
LANMSGDD.OS2  \IBMCOM
PROTMAN.OS2   \IBMCOM
LTO.MSG       \IBMCOM
LT2.MSG       \IBMCOM
PRO.MSG       \IBMCOM
LANMSGDL.DLL  \IBMCOM\DLL
IBMTOK.OS2    \IBMCOM\MACS
NETBIND.EXE   \IBMCOM\PROTOCOL
```

- **NetBIOS files**

  For NetBIOS support, the following files must be copied from a working NetBIOS system to disk 1:

```
Filename      Found in
----------------------
NETBEUI.OS2   \IBMCOM\PROTOCOL
NETBIOS.OS2   \IBMCOM\PROTOCOL
```

- **386-HPFS files**

  Optionally, if you are using Warp Server Advanced with 386-HPFS, add the following files to disk 1 to include 386-HPFS support:

```
Filename      Found in
----------------------
386-HPFS.IFS  -IBM386FS
386-HPFS.INI  -IBM386FS
HFS.MSG       -IBM386FS
BOOTSH.EXE    -IBM386FS
BSH.MSG       -IBM386FS
BSHH.MSG      -IBM386FS
```

Step 4: Modify CONFIG.SYS and CMD Files: Make the following changes to the CONFIG.SYS file on disk 1:

- **References on CONFIG.SYS**

  Remove any reference in the CONFIG.SYS to the following files:

```
XDFLOPPY.FLT
MOUSE.SYS
```

- **Paths**

  Change the three path statements so that they reference the A: drive:

```
LIBPATH=.;\;A:\;
SET PATH=.;\;A:\;
SET DPATH=.;\;A:\;
```

- **Initialization**

  To correctly execute the STARTUP.CMD, include the following in your CONFIG.SYS file:

  ```
  PROTSHELL=SYSINST1.EXE
  SET OS2_SHELL=CMD.EXE /K STARTUP.CMD
  ```

  Note on 386-HPFS Only

  To correctly install the 386-HPFS and execute the STARTUP.CMD, include the following lines in your CONFIG.SYS file instead:

  ```
  PROTSHELL=BOOTSH.EXE CMD.EXE /K STARTUP.CMD
  IFS=386-HPFS.IFS A:\386-HPFS.INI /AUTOCHECK:
  SET OS2_SHELL=CMD.EXE
  ```

- **Device drivers**

  All device drivers copied to disk 1 must be referenced at startup time. Add the following lines to the bottom of CONFIG.SYS:

  ```
  REM *** Protocol/LAN/Vdisk Drivers ***
  DEVICE=\VDISK.SYS 4069,,
  DEVICE=\LANMSGDD.OS2 /I:A:\
  RUN=\LANMSGEX.EXE
  DEVICE=\PROTMAN.OS2 /I:A:\

  REM *** Network Adapter Driver ***
  DEVICE=\IBMTOK.OS2

  REM *** NetBIOS Drivers ***
  DEVICE=NETBEUI.OS2
  DEVICE=NETBIOS.OS2

  REM *** Netbind ***
  RUN=\NETBIND.EXE
  ```

Step 5: Create Disk 2: To create disk 2, use a temporary directory. Collect the required files on it and build a ZIP file from them. The resulting ZIP file must be copied to disk 2, along with the corresponding UNZIP utility. Disk 2 contains compressed versions of NetBIOS files, OS/2 utilities, and CID Code Server files.

- **Create a temporary directory**

To collect all necessary files, create a working directory, for example, C:\TEMPADSM.

- **NETBIOS files**

  To support NetBIOS you must include this file:

  ```
  ACSNETB.DLL
  ```

  Copy the file from a working NetBIOS system to temporary directory \TEMPADSM.

- **Utilities**

  The following utilities can be useful when working on a damaged workstation. You can add more; the limit is the free space available on disk 2.

  Copy these files to temporary directory \TEMPADSM.

  ```
  FDISK.COM    - For repartitioning if necessary
  FORMAT.COM   - For reformatting if necessary
  LABEL.COM    - For changing volume names
  CHKDSK.COM   - For repairing filesystem damage
  UHPFS.DLL    - Required for HPFS partition work
  ATTRIB.EXE   - For altering file attributes
  MAKEINI.EXE  - For repairing/rebuilding the OS/2 INI file
  XCOPY.EXE    - For copying files
  INI.RC       - Seed file for MAKEINI
  INISYS.RC    - Seed file for MAKEINI
  LOCK.RC      - Seed file for MAKEINI
  SYSINSTX.COM - For bootstrap sector initialization
  TEDIT.EXE    - An text editor
  OSO001.MSG   - OS/2 Message repository
  ```

  – **CID Code Server files**

    To run the CID Code Server, include the CID Code Server files as follows:

Extracting the LAN CID Utilities Files

Extract the CID Code Server files from the LAN CID Utilities (LCU) included with OS/2 Warp Server on MPTS diskette 5 or in the Warp Server CD-ROM. Use the following sample:

Create a temporary directory:

```
CD C:
MD TMPLCU
```

Change to the directory you have created

```
CD TMPLCU
```

To extract the files from MPTS diskette 5 in your A: drive to temporary directory C:\TMPLCU, execute the following commands:

```
PKUNZIP2 A:\SRVIFS\SRVIFS.ZIP
    COPY A:\README.UTL
```

To extract the files from the Warp Server CD-ROM in your X: drive to temporary directory C:\TMPLCU, execute the following commands:

```
PKUNZIP2 X:\CID\SERVER\IBMLS\IBM5OON5\SRVIFS.ZIP
    COPY X:\CID\SERVER\IBMLS\IBM5OON5\README.UTL
```

Now the required files are available on your TMPLCU directory.

Read the README.UTL file, which includes technical information about MPTS.

Copy the following files to the C:\TEMPADSM directory:

```
Filename      Found in
----------------------
SERVICE.EXE  -TMPLCU
XI1.MSG      -TMPLCU
XI1H.MSG     -TMPLCU
RESCUE1.INI  -See B.8, "RESCUE1.INI" on page 277.
```

(The RESCUE.INI contains the initialization parameters for SERVICE.EXE.)

– **Build the zip file**

If you use the PkZip2 and PKUnZip2 utilities with C:\TEMPADSM as the temporary directory, execute the following commands to build the zip file on disk 2:

```
C:
CD C:\TEMPADSM
PKZIP2 ADSMPACK.ZIP *
```

If you are using the ZIP and UNZIP utilities, execute the following commands to compress all of the files you gathered together into a file named ADSMPACK.ZIP:

```
C:
CD C:\TEMPADSM
ZIP ADSMPACK.ZIP *
```

Copy this file to disk 2.

- **Copy the decompression utility**

  Copy the corresponding decompression program (PKUNZIP2.EXE or UNZIP.EXE) to disk 2. If you use InfoZip's UNZIP.EXE, you will have to copy the NLS.DLL file from your \OS2\DLL subdirectory onto disk 2.

Make sure you edit PART2.CMD to specify which decompression utility you will be using.

6.2 Setup of the OS/2 Peer Recovering Workstation

The OS/2 CID Peer workstation selected to do the recovery must be configured to run the NetBIOS communication protocol. This allows the CID Client Redirection program, SRVATTCH.EXE, to attach the disk drives on the failing workstation. Also the recovery machine must be able to manage the file system used by the failing machine.

6.2.1 Preparation of the Recovery System

This simple process has only two steps:

1. Install some files in the OS/2 CID Peer workstation.
2. Add some lines to your CONFIG.SYS file.

Step 1: Install the CID Client Redirection Files:

These files are already available on the TMPLCU directory that you created when you built the bootable diskettes. You may copy the files from there to the OS/2 CID Peer workstation.

Copy the following files from the TMPLCU directory to the root directory of the C drive on the OS/2 CID Peer machine.

```
Filename      Found in
----------------------
SRVIFS.SYS   -TMPLCU
SRVIFSC.IFS  -TMPLCU
SRVATTCH.EXE -TMPLCU
XI1.MSG      -TMPLCU
```

```
XI1H.MSG      -TMPLCU
```

For simplicity we used the root directory on C drive, but you can use a different one; remember to change your CONFIG.SYS file accordingly.

Step 2: Edit the CONFIG.SYS File

First, make a backup copy of your CONFIG.SYS file. Then use an editor to add the following lines to the end of the CONFIG.SYS:

```
REM --- CID Client Redirection ---
DEVICE=C:\SRVIFS.SYS
IFS=C:\SRVIFSC.IFS SERVER1
```

You need to reboot your OS/2 CID Peer workstation to activate these lines.

6.2.2 Additional Preparations

In your preparations for the disaster, we recommend that you additionally collect and save information about the ADSM client platform to aid in any future postdisaster re-creation of the hardware environment.

6.3 Postdisaster Recovery

In this section we show how we recovered from a disaster using the bootable diskettes, the OS/2 CID Peer workstation, and the information saved before the disaster.

We simulated a disaster by installing a new blank disk drive so that the machine would no longer boot and then followed this procedure:

6.3.1 Rebuild the Hardware Environment

Retrieve information about the machine to help re-reate the hardware environment of the destroyed ADSM client. The new replacement machine must have a similar configuration as the system files recovered from ADSM will reference it.

If DRM had been used as the repository for this type of information, you could retrieve it by issuing the appropriate ADSM queries to the ADSM server. For examples of these queries, see 1.3.6, “Disaster Recovery Manager” on page 18.

6.3.2 Booting the Recovery System

Use the diskettes to boot the replacement hardware and prepare the workstation to run the CID Code Server. Follow these steps:

1. Boot the machine with disk 0, until the blue screen asking for disk 1 appears.
2. Insert disk 1 and press <ENTER>. Look for the messages reporting successful LAN and NetBIOS startup:

```
SYS0318: Message file OSO001.MSG cannot be found for message  1467.

IBM OS/2 LANMSGDD ( 04/26/95 ) 2.01 is loaded and operational.
IBM OS/2 LAN Protocol Manager

IBM OS/2 NETBEUI 5.00.0
NETBEUI: Using a 32-bit data segment
IBM OS/2 NETBIOS 4.0
Adapter 0 has 254 NCBs, 254 sessions, and 41 names available to NETBIOS
applications
NETBIOS 4.0 is loaded and operational.
```

Message SYS0318

The message SYS0318 is reporting that there is no repository file available to retrieve the contents of message 1467. The format of the message 1467 is shown below:

```
SYS1467: VDISK Version 2.1 Virtual disk ***
disk Size:          4000 KB
Sector Size:        512
Directory Entries:  64
```

After a few moments the screen is cleared, and you will see:

```
ADSM BOOTABLE RECOVERY STARTED........
*********************************************
 .
Searching for a VDISK
Vdisk Found as drive (E:\)
 .
Copying files to drive (E:\)
 .
Unpacking file to VDISK
Wait for all diskette activity to stop, (background processes..)
Remove diskette 1 from the drive, and insert diskette 2 and then
Press any key when ready  . . .
```

3. Wait for all activity to stop, remove disk 1, insert disk 2, and press <ENTER>. Wait for the message requesting disk 1 again:

```
Working...
PKUNZIP (R) FAST!  Extract Utility  Ver. 1.09-OS/2 Prot Mode 1-15-91
Copr. 1989-1991 PKWARE Inc. All Rigths Reserved PKUNZIP/h for help
PKUNZIP Reg. U>S> Pat. an Tm. Off.     IBM LICENSED VERSION


Searching ZIP: A:ADSMPACK.ZIP
  Exploding: acsnetb.dll
  Exploding: ATTRIB.EXE
  .
  .
  .
  Exploding: XI1.MSG
  Exploding: XI1H.MSG
Done...
Please remove diskette 2 from the drive, and insert diskette 1 and then
Press any key when ready  . . .
```

4. After you remove disk 2, insert disk 1, and press <ENTER>, the tiny editor TEDIT.EXE shows the contents of RESCUE1.INI, which contains the initialization parameters for the SERVICE.EXE program.
5. You must define as many ALIAS lines as drives you will be restoring. The drive being referenced on an ALIAS statement must exist, or you will get an error.

   Below is a sample of the screen that you will be see:

```
==== Top of File ====
*
* RESCUE1.INI file  used by SERVICE.EXE
* ------------------------------------
* Edit the values or add more ALIAS sentences if required.
* Then, save to continue.
*
Name=RESCUE1
GroupName=yes
Adapter=0
MaxClients=1
Path=C:\
PermitWrite=no
MaxFiles=100
ClientWorkers=6
Alias=readwrite,single,DISKC,C:\
Alias=readwrite,single,DISKD,D:\
==== End of File ====


c:\tempadsm\rescue1.ini                                        1     1
F1=Help F2=Save F3=Quit F4=File F5=Cmd F7=Name F8=Edit F9=Undo F10=Next
```

The sample file shown defines two ALIASes. In this sample, the file is saved without changes because it is correct to work with the C and D drives to be recovered. To save, press PF4.

6. After the last messages shown below, the OS/2 prompt appears. At this point the CID Code Server can be started, or some preliminary tasks using the OS/2 utilities can be performed; for example, setting up the new hard drive.

```
Initialization Complete
 .
To Start the CODE Server, enter:
 .
SERVICE /INI=RESCUE1

E:\
```

6.3.3 Setting Up a New Hard Drive

The utilities required to set up the new hard drive are ready to use on the virtual drive. Depending on the operating system being recovered, you may have to use other utilities from the particular operating system diskettes.

- Parition the hard drive, using FDISK, to match the size and type as recorded before the disaster.
- After partitioning the hard drives, FDISK requires that the machine be rebooted. Use disk 0 to reboot. Disk 1 and disk 2 will be requested, and the OS/2 prompt appears.
- To format the partitions to the file system type used previously, use the following commands:
  - For OS/2 use FORMAT and SYSINSTX commands:

    ```
    FORMAT C: /FS (:HPFS or FAT as required)
    FORMAT D: /FS (:HPFS or FAT as required)
    SYSINSTX C:  - only C requires the boot sector
    ```

  - For DOS/Windows the easiest way to format and tranfer the boot record and system files at the same time is to boot from a DOS diskette (make sure the FORMAT.COM file is included in the diskette) and enter:

    ```
    FORMAT C: /S    - only C requires the /S switch
    FORMAT D:
    ```

    Assign to the partition the **same** label previously used for the drives. ADSM needs the labels on the drives to identify the ADSM filespaces.

Also to make the new disk bootable, make sure you install the Boot Sector and related system files.

You MUST use a diskette with the ***SAME*** VERSION and BRAND of DOS as was used in the original damaged drive.

– For Windows95 use the Windows Startup disk to boot, then enter:

```
FORMAT C: /S    - only C requires the /S switch
FORMAT D:
```

After this process, the drive(s) are ready to use. Now boot again with the CID recovery diskettes and continue with the restoration steps.

6.3.4 Restore from the ADSM Backup

In this section we describe how to attach the failed machine′s drives to the CID Peer so they may be restored using an ADSM client.

6.3.4.1 Restoring the Whole System

To restore the whole system from the ADSM backup, do the following:

- To activate the CID Code Server on the machine to be recovered (on the damaged workstation), issue the following command:

  ```
  SERVICE /INI=RESCUE1
  ```

  The CID Code Server will be activated, and you will see the following screen:

  ```
  E:\service /ini=rescue1
  RESCUE1 Server is active, Version 1.32.2
  ```

  Note: We sometimes had to repeat this command if nothing happened after a few seconds.

  At this point, the CID Code Server is active on the machine to be recovered. All other activities to complete the restoration have to be performed on the OS/2 CID Peer workstation.

  The OS/2 CID Peer workstation is ready to use the disk drives on the failing machine. All you have to do is issue the SRVATTCH command to attach the drives through the LAN, using the NetBIOS facilities.

- In an OS/2 window issue the following commands:

  ```
  SRVATTCH X: \\RESCUE1\DISKC
  SRVATTCH Y: \\RESCUE1\DISKD
  ```

  where RESCUE1 is the name of the CID Code Server, and DISKC and DISKD are the ALIASes defined in the RESCUE1.INI file.

New disks available

After the command completes successfully, two new disks are available in the OS/2 CID Peer workstation:

The new X drive is the C drive on the damaged machine.

The new Y drive is the D drive on the damaged machine.

To verify that you are accessing the drives, issue a DIR command against the new X and Y drives.

- On the OS/2 CID Peer workstation, open an OS/2 window and start the ADSM client program using the same ADSM nodename as the nodename of the failing machine. In our case we issued the following command:

  ```
  DSMC -NODENAME=CANDEMAS
  ```

  where CANDEMAS is the ADSM nodename of the failing machine.

  Be careful that you connect to the ADSM server using the nodename of the failing workstation so that you do not overwrite the local drives.

  At this point, you are connected to the ADSM server and ready to start the restore process.

- At the ADSM prompt, issue the following command:

  ```
  RESTORE -SUBDIR=YES -REPLACE=ALL {OS2}\* X:\
  ```

  We used the ***filespace name*** in the restore command because it is independent of the drive labels on the OS/2 CID Peer workstation. ADSM responds to the commands with the following:

```
C:\ dsmc -nodename=candemas
ADSTAR Distributed Storage Manager
Command Line Backup Client Interface - Version 2, Release 1, Level 0.0
(C) Copyright IBM Corporation, 1990, 1995, All Rights Reserved.

dsmc> restore -subdir=yes -replace=yes {OS2}\* x:\
Restore function invoked.

Please enter password for node "CANDEMAS": ********

Session established with server ADSM: AIX-RS/6000
  Server Version 2, Release 1, Level 0.9
  Server date/time: 09/18/1996 11:13:01   Last access: 09/18/1996 11:00:4

ANS4166I ***** Examined 1000 files *****
ANS4166I ***** Examined 2000 files *****
Restored directory X:\ADSM\
Restored directory X:\ADSM\API\
Restored directory X:\BOOKS\
Restored directory X:\Desktop\
Restored directory X:\Desktop\ADSM Client\
Restored directory X:\Desktop\IBM Internet[Connection for OS!2\
      .                                    .
      .                                    .
      .                                    .
Restoring      522,877 C:\tcpip\umail\viewcli.dll --> X:\tcpip\umail\view
cli.dll ......... Done
Restoring        1,957 C:\IBMLAN\NETPROG\RDRHELP.200 --> X:\IBMLAN\NETPRO
OG\RDRHELP.200 . Done
Restoring        1,536 C:\IBMLAN\NETSRC\OS2\LIB\UPM32.LIB --> X:\IBMLAN\N
ETSRC\OS2\LIB\UPM32.LIB . Done

Restore processing finished.
dsmc>
```

Repeat the process for the Y drive, issuing this command:

```
RESTORE -SUBDIR=YES -REPLACE=YES {PROJECT}\* Y:\
```

After you complete the restore, reboot the recovered machine.

6.3.4.2 Restore Any Workstation-Dependent Information

Now any information required additionally to the ADSM restore should be recovered (ACPs in LAN or Warp Server Advanced versions - see Chapter 4, “OS/2 LAN Server: Bootable, Direct Recovery” on page 61 and Chapter 5, “OS/2 Warp Server Recovery from an OS/2 CID Peer Workstation” on page 83 or long file names under Windows 95- see Chapter 8, “Windows 95 Recovery” on page 137).

6.3.4.3 Verifying the Postdisaster Restoration

An optional step as recovery verification (see 5.2, “Predisaster Preparation” on page 84). The predisaster snapshot could be compared to the

postdisaster recovery environment to ensure that the restoration was complete.

Chapter 7. DOS/Windows Version 3.1 Recovery

In this chapter we explain how to use bootable diskettes to recover a DOS/Windows Version 3.1 client environment that uses TCP/IP to communicate with its ADSM server. We review the kind of information to back up in preparation for a disaster, explain how to create the bootable diskettes, and discuss how to use the bootable diskettes in conjunction with the saved information to recover after a disaster.

Note: The bootable diskettes method requires the ADSM DOS backup-archive client, even if you usually use the ADSM Microsoft Windows backup-archive client to handle your daily ADSM duties.

It is also possible to use configuration, installation and distribution (CID) peer recovery for this platform. Refer to Chapter 6, “Recovery of OS/2 and Windows from an OS/2 CID Peer” on page 107 for information about using CID peer recovery for DOS clients.

7.1 Product Overview

The DOS operating system was released when the PC was first introduced in 1982. DOS has been updated several times since then. Windows was released as an add-on product to DOS to help people using their home computers. DOS together with Windows 3.1 constitutes the most common operating system in use today.

The FAT file system was originally designed to support floppy disks. As hard disks, CD-ROMs, and networks have become more and more common, the FAT file system has been modified. FAT has only limited support for error correction and allows very brief file names. However, FAT is still the most common file system used on various PC operating systems today.

DOS is a single-user operating system, so it has no security mechanisms.

7.2 Predisaster Preparation

The disaster we are preparing for is the total and catastrophic loss of the ADSM client, where provision has to be made to restore everything from the bare metal up. If our disaster recovery preparations can cover this worst case scenario, we can assume that they will also be able to handle recovery from lesser disasters.

In this section we discuss the information to collect and save before a disaster to enable a bare metal restore.

7.2.1 ADSM Backups

If recovery of the operating system is to be from ADSM, a full backup that includes system files must be taken. This is not the default. The system files will of course be specific to the configuration of the machine being backed up. Figure 25 shows the predisaster normal backups being taken.

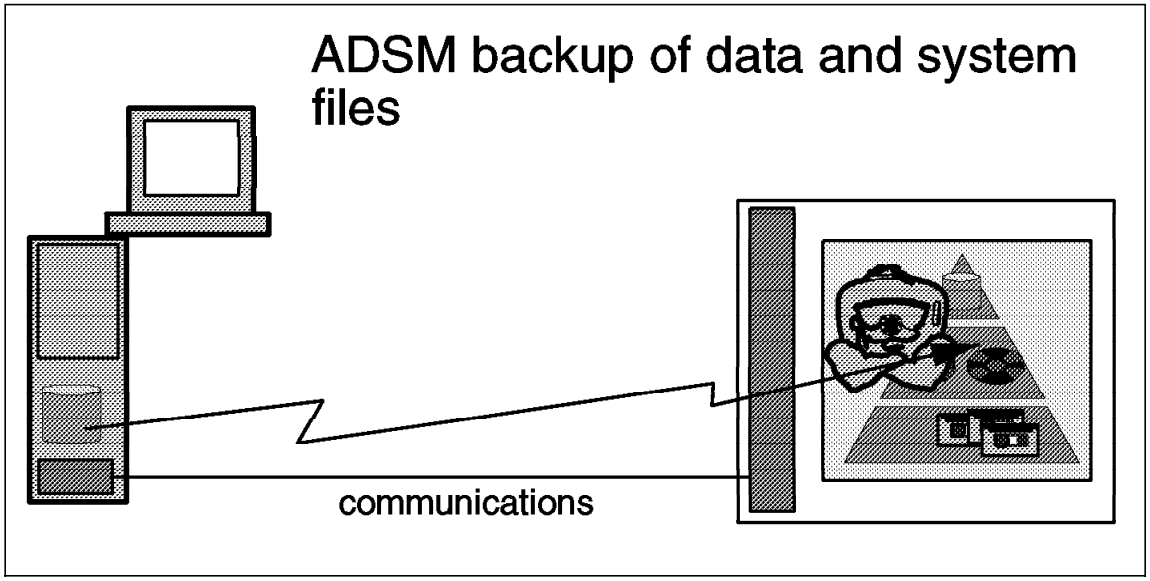


Figure 25. Full ADSM Backup Including System Files

We recommend that you use the following options for the ADSM backup that you will use for the ADSM bare metal restore:

- Set the **Copy Serialization** parameter in the **Backup Copy Group** definition to **Shared Static** This setting allows only those files not being modified to be included in the ADSM backup (preventing a ″fuzzy″ backup). When using this setting, it is best to schedule the ADSM backup during a period of low utilization of the ADSM client. Because this ADSM backup is oriented to provide an image of the workstation to be used in case of disaster, all applications and subsystems running on the machine should be closed before the backup, so that you have the fewest number of open files.
- Because we depend on the existence of an ADSM backup that would provide full restoration of the ADSM client being recovered, we recommend that the ADSM options file, **DSM.OPT**, only EXCLUDE the SWAPPER.DAT and the EA DATA.SF files. This recommendation implies that you include the operating system software on the C: drive in the ADSM backup. The bootable diskettes will provide only a skeleton version of DOS that will enable the ADSM client to function. The

assumption is that the newly booted system with the ADSM client will be used to restore the rest of the DOS system from an ADSM backup done *for that client.* This may be contrary to your current backup policy (you may currently deliberately EXCLUDE the C: drive from your ADSM backups). This backup should also include empty directories.

7.2.2 Operating Environment of the ADSM Client

In preparation for disaster recovery we recommend that you collect and save offsite the information listed below in addition to the ADSM backup data. Depending on your installation, you could save this information by using the DRM feature, or you could save it on hardcopy stored offsite. The way in which you save the information is not as important as ensuring that it is saved **somewhere** where it can be easily retrieved along with the client recovery media when a disaster occurs.

- **Hardware configuration**

  Keep information about machine type, bus type, hard disk attachment, and of course, the type of network adapter used. Collect any such information that will help you re-create the hardware setup of the ADSM client that has been destroyed in a disaster. If you are using a PS/2, for instance, you may also include information about where to find copies of the associated PS/2 hardware reference diskettes in case you find yourself needing to replace a hard disk.

- **Partitioning drives**

  Record how the hard drives are partitioned and labeled. You can collect this information by using the Fdisk command. To do the restore ADSM has to know the hard drive label. We recommend that you define hard drive labels that include the drive letter, to make it easier to determine which ADSM filespace should be restored to which drive at disaster recovery time.

- **Communication details**

  Specific information about your installation communications setup (for example, TCP/IP addresses of the ADSM client and server; SUBNET, ROUTE, and DOMAIN name; TCP/IP port number of the ADSM service; and ADSM node name). This information could be customized on the bootable diskettes. However, if one set of bootable diskettes will be used to service many clients, you may want to store this data for each individual client (using offsite hardcopy or DRM).

Optional: Statistics for Postdisaster Recovery Verification

You may want to gather and save information that can be used after a disaster recovery test once the restore process is completed, to validate that all information has indeed been restored correctly. Each installation will have its own ideas about the best way to verify that the recovery is complete. Some possible sources of information for recovery verification are:

- ADSM statistics at the end of the backup, such as the Number of Objects Inspected, would give a tally of the directories and files on the client being backed up.
- CHKDSK command output for each backed up disk

  Run CHKDSK for each drive being backed up and record:

  - *X* number of kilobytes used in *A* number of directories
  - *Y* number of kilobytes used in *B* number of user files
  - *Z* number of kilobytes used in extended attributes

  For FAT drive records:

  - *X* number of kilobytes used in *A* hidden files
  - *Y* number of kilobytes used in *B* number of directories
  - *Z* number of kilobytes used in *C* user files
- DIR command output

  Collect the output of the DIR /A /S command in a file for each drive. After disaster recovery testing, use the output to compare the files available before the test. Utilities such as the AIX DIFF program could be used for this kind of comparison.
- Other test scripts used during your installation's periodic disaster recovery tests.

7.2.3 Creating the Bootable Diskettes

In this section we describe a method to create bootable diskettes for DOS/Windows Version 3.1. The rationale for creating these diskettes is that, after a disaster, they can be used to quickly boot a replacement machine with the minimal operating system, communications, and ADSM software necessary to begin file restoration using the ADSM client and server. Normal ADSM recovery can then be used to restore the remainder of the predisaster client environment.

7.2.3.1 Assumptions

These instructions apply to MS-DOS or PC-DOS machines with or without Windows 3.1 that use a token ring and TCP/IP. Modifications may be necessary for this technique to work in environments using other network adapters, hard disk controllers, and so on.

The instructions apply to the following products:

- PC-DOS or MS-DOS with MS-Windows 3.1
- IBM TCP/IP Version 2.1 for DOS
- ADSM Version 1, Release 2 client for DOS
- ADSM Version 2, Release 1 client for DOS
- Any ADSM server that uses TCP/IP

A complete ADSM backup as described in 7.2, “Predisaster Preparation” on page 125 should be available at the ADSM server, and the restore should be done to a hardware configuration similar to that of the original ADSM backup-archive client machine.

7.2.3.2 Configuration Used to Test This Technique

We tested this technique on the following configuration:

- Personal Computer 750 with 32 MB of RAM
- 16 Mbps token-ring attachment
- 1.6 GB IDE-attached hard drive, partitioned as follows:
  - C drive: FAT primary partition, 200 MB, labeled ″DRIVE-C″
- PC-DOS 7.1 with MS-Windows 3.1
- IBM TCP/IP Version 2.1.1.4 for DOS
- ADSM for Windows 16-bit Version 2, Release 1, Level 0.3 client
- ADSM for DOS Version 2, Release 1, Level 0.3 client
- ADSM/AIX Version 2, Release 1, Level 0.2 server code

To use this technique you will need:

- Two blank formatted 1.44 MB diskettes
- If you are using PS/2 hardware, the associated hardware reference diskettes may be useful.

7.2.3.3 Step-by-Step Instructions

Step 1: Create the Stand-Alone Diskettes: Format two 1.44 MB diskettes. Mark them disk 0 and disk 1.

Use the following command to make disk 0 bootable:

```
SYS A:
```

Step 2: Edit the Stand-Alone Diskettes to Add Files: Once you create the stand-alone diskettes, some changes have to be made to them:

- **Add DOS files**

  Here are the DOS files you have to copy to or create on disk 0:

Filename	Found in
ATTRIB.EXE	\DOS
CHKDSK.COM	\DOS
EMM386.EXE	\DOS
Fdisk.COM	\DOS
FORMAT.COM	\DOS
HIMEM.SYS	\DOS
LABEL.COM	\DOS
SYS.COM	\DOS
CONFIG.SYS	See B.9, "CONFIG.SYS" on page 278
AUTOEXEC.BAT	See B.10, "AUTOEXEC.BAT" on page 279

- **Create an IBMDOS directory on disk 0**

  To separate the LAN support and TCP/IP files from the other DOS utilities, create an IBMDOS directory, IBMDOS, on disk 0.

- **Add LAN support and TCP/IP files**

  You must have the support layer necessary to operate your network card at the hardware level. Here is a list of files you have to add to \TCPIP on disk 0. Next to each filename is a hint as to where to find them on a working LAN-attached system.

Filename	Found in
ARP.EXE	\IBMDOS\BIN
DOS16M386	\IBMDOS\BIN
DOSTCP.SYS	\IBMDOS\BIN
IBMTOK.DOS	\IBMDOS\BIN
IBMTOK.NIF	\IBMDOS\BIN
IFCONFIG.EXE	\IBMDOS\BIN
INET.EXE	\IBMDOS\BIN

```
INET.SYM      \IBMDOS\BIN
LT2.MSG       \IBMDOS\BIN
NETBIND.COM   \IBMDOS\BIN
NETSTAT.EXE   \IBMDOS\BIN
PING.EXE      \IBMDOS\BIN
PROTMAN.DOS   \IBMDOS\BIN
PROTMAN.EXE   \IBMDOS\BIN
PROTOCOL      \IBMDOS\BIN
PROTOCOL.INI  \IBMDOS\ETC
RESOLV        \IBMDOS\ETC
ROUTE.EXE     \IBMDOS\BIN
```

Note: Depending on your setup, you may have to replace IBMTOK.DOS, IBMTOK.NIF, and LT2.MSG with whatever NDIS driver is appropriate for your network adapter. IBMTOK.DOS works merrily for most variations of IBM token-ring adapters. For other adapters, you have to determine which NDIS driver you are currently using. If you do not know which driver you use, try looking in the following places:

- PROTOCOL.INI file. All of your protocols should be bound to one driver. The internal name of the driver (for example, IBMTOK$) should be similar to the file name (for example, IBMTOK.DOS).
- Look through CONFIG.SYS. Some drivers, such as IBMETHRN.DOS, jump right out at you.

- **Add ADSM client files**

  Here are the ADSM files that you have to copy or create on disk 1.

```
Filename      Found in
------------------------
DSCAMENG.TXT  \ADSM
DSMCIBM.EXE   \ADSM
DSMC.HLP      \ADSM
DSM.OPT       See B.11, "DSM.OPT" on page 279
```

Step 3: Create the CONFIG.SYS File: Entries need to be made to the CONFIG.SYS file on disk 0:

- **Memory management statements**

  These three statements need to be made so that DOS manages its available memory well:

```
DOS=HIGH,UMB
DEVICE=A:\HIMEM.SYS
DEVCIE=A:\EMM386.EXE NOEMS
```

- **Initialization**

  Ensure that the following lines are included:

```
FILES=50
BUFFERS=30
STACKS=9,256
```

- **Device drivers**

  All of the device drivers copied to disk 0 must be referenced at startup time. Add the following lines to the bottom of CONFIG.SYS:

```
DEVICEHIGH=A:\TCPDOS\PROTMAN.DOS /I:A:\TCPDOS
DEVICEHIGH=A:\TCPDOS\DOSTCP.SYS
DEVICEHIGH=A:\TCPDOS\IBMTOK.DOS
```

Step 4: Create the AUTOEXEC.BAT File: Add the following entries to the AUTOEXEC.BAT file on disk 0:

- **Set the ETC directory**

  To tell TCP/IP where to find the PROTOCOL.INI and the resolve file add:

```
set etc=a:\tcpdos;
```

- **Paths**

  The path statement should refer to \ and \TCPDOS

```
path=a:\;a:\tcpdos;
```

- **TCP/IP configuration**

  To set up a working TCP/IP environment you have to add the following lines to your AUTOEXEC.BAT file (substitute your own TCP/IP address, NETMASK, and ROUTE):

```
netbind

inet

route -fn
arp -dan

ifconfig nd0 129.33.160.154 netmask 255.255.255.0 up

route add default 129.33.160.254
```

Step 5: Create the DSM.OPT File: Add these entries to the DSM.OPT file on disk 1:

- **Set the communication method**

  To set up a working ADSM environment, you have to add the following lines to your DSM.OPT file (substitute your own TCP/IP server address and port number):

```
COMMMETHOD          TCPIP
TCPSERVERADDRESS    129.33.160.100
TCPPORT             1500
TCPWindowsIZE       4
TCPBUFFSIZE         4
```

- **Set the NODEname**

  Do not forget to set the node name, for example:

  ```
  NODENAME            KARIN
  ```

7.3 Postdisaster Recovery

In this section we describe how to recover from a disaster to the DOS/Windows Version 3.1 ADSM client by using the information you saved before the disaster (described in 7.2, “Predisaster Preparation” on page 125) and the bootable diskettes you created (described in 7.2.3, “Creating the Bootable Diskettes” on page 128.)

To simulate a disaster, we installed a new blank hard drive on our DOS/Windows Version 3.1 ADSM client, so that our machine would no longer boot and then followed this procedure:

7.3.1 Rebuild Hardware Environment

Retrieve information about the DOS/Windows Version 3.1 machine to help re-create the hardware environment of the destroyed ADSM client. The new replacement machine must have a similar configuration.

If DRM had been used as the repository for this type of information, you can retrieve it by issuing the appropriate ADSM queries to the ADSM server.

7.3.2 Boot the Recovery System

Use the DOS/Windows Version 3.1 bootable diskettes to boot the replacement hardware and prepare for ADSM file recovery. Follow these steps:

1. Boot the machine with disk 0 and wait until the command prompt appears.
2. Remove disk 0 and insert disk 1. At this point the ADSM restore can be started, or some preliminary tasks using the DOS utilities can be performed. For example, repartitioning a new hard disk using the Fdisk utility.

7.3.3 Restore from the ADSM Backup

At this point you are ready to begin restoration of files from the ADSM server. Some possible recovery scenarios are described below:

7.3.3.1 Restoring the Whole System

Note: ADSM identifies your drives by their volume name and expects that your replacement drive will have the same setup and label as the original. The ADSM QUERY FILESPACE command tells you which volume labels ADSM expects to see.

To restore the whole system from the ADSM backup, invoke the ADSM command line client and issue the following command:

```
DSMCIBM  RESTORE C:\* -SUBDIR=YES -REPLACE=YES
```

ADSM responds to this command with the following:

```
ADSTAR Distributed Storage Manager
Command Line Backup Client Interface - Version 2, Release 1,Level 0.0
(C) Copyright IBM Corporation, 1990, 1995, All Rigths Reserved.

dsmc> RESTORE C:\* -SUBDIR=YES -REPLACE=YES
RESTORE function invoked.

Please enter password for node "SERVER1": *******

Session established with server ADSM: AIX-RS/6000
  Server Version 2, Release 1, Level 0.2
  Data compression forced on by the server
  Server date/time: 08:30:1996 17:53:11  Last access: 08/30/1996 17:47:55

Restoring            0 C:\TCPCFG.LOG --> C:\TCPCFG.LOG  Done
Restoring          388 C:\AUTOEXEC.01 --> C:\AUTOEXEC.01 . Done
Restoring          368 C:\AUTOEXEC.MGA --> C:\AUTOEXEC.MGA . Done
Restoring        4,278 C:\CONFIG.BK1 --> C:\CONFIG.BK1 . Done
        .        .
        .        .
        .        .
Restore processing finished.
```

7.3.3.2 Restoring a File

Perhaps you have deleted the CONFIG.SYS or some other important file, and DOS will not start. Assuming you have included these elements in a recent ADSM incremental backup, restore the file using ADSM:

```
DSMCIBM RESTORE C:\dirname\filename.ext -REPLACE=ALL
```

7.3.3.3 Restoring a Directory

If you have just destroyed an important directory like C:\DOS, and assuming that you have included it in your ADSM incremental backup, restore the files using ADSM:

```
DSMCIBM RESTORE C:\DOS\* -REPLACE=ALL
```

7.3.3.4 Restoring an Entire Directory Structure

Perhaps you deleted an entire directory structure by using an ill-conceived command like DELTREE C:\Windows. Assuming you have backed up this structure, you can restore it using ADSM:

```
DSMCIBM RESTORE C:\Windows\* -REPLACE=ALL -SUBDIR=YES
```

7.3.3.5 Rebooting the System

After doing any of the above, reboot your system.

7.3.3.6 Verify the Postdisaster Restoration

At this point, if part of a disaster recovery test, you would use any statistics you saved with your ADSM backups and bootable diskettes to verify that they are comparable to those you receive after your recovery is complete.

Chapter 8. Windows 95 Recovery

In this chapter we discuss how a Windows 95 system may be prepared for disaster recovery. We cover the problems specific to Windows 95 and how these may be overcome to produce a disaster recovery plan utilizing ADSM backup/restore.

We discuss the kind of information that should be backed up in preparation for a disaster, how to create bootable diskettes for recovery, and how to use the bootable diskettes in conjunction with the previously saved information to recover a Windows 95 environment after a disaster.

8.1 Product Overview

Windows 95 is a personal computer operating system that provides 32-bit multitasking and performance while retaining backward compatibility with earlier DOS- and Windows-based applications.

Although Windows 95 is based on the architectural design of Windows Version 3.1, it includes many improvements over the previous operating system:

- Protected mode 32-bit operating system with no DOS layer
- Preemptive multitasking
- 32-bit installable file systems including VFAT, CDFS, and network redirectors
- 32-bit kernel and device drivers

Figure 26 on page 138 shows the basic architecture of Windows 95.

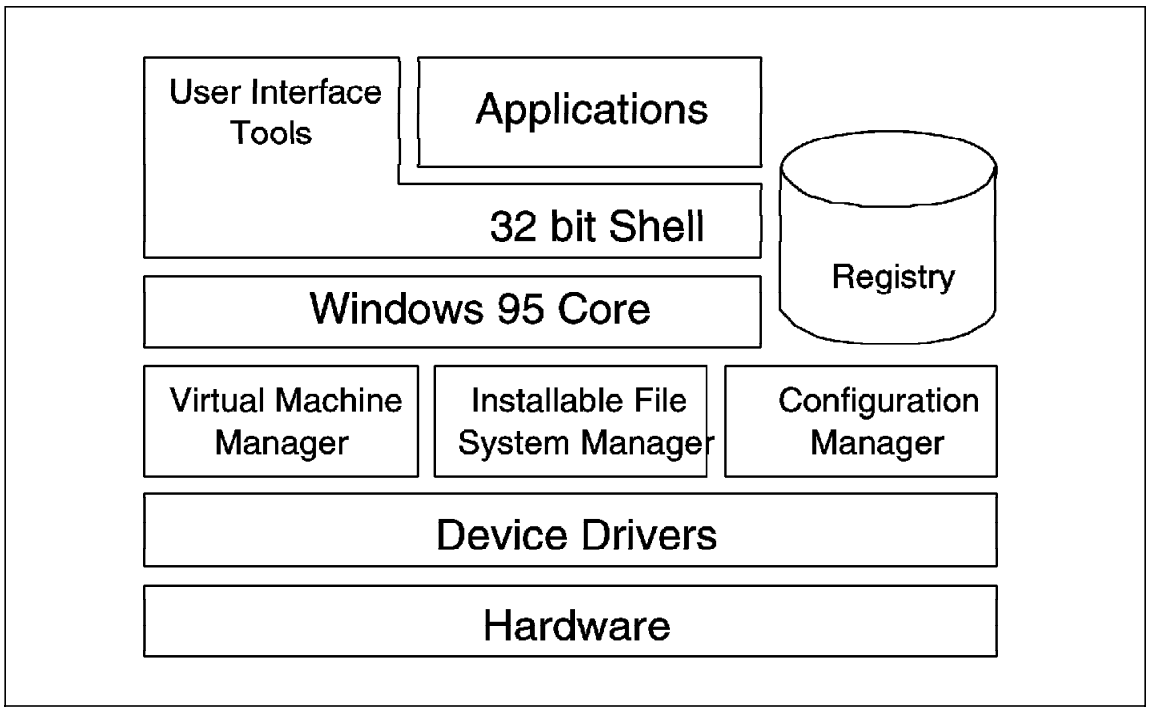


Figure 26. Windows 95 System Architecture

One of the primary changes in Windows 95 is the introduction of the system *registry* which is effectively a hierarchical database of information about the system, its devices,and users. The registry replaces all of the traditional startup and configuration files (such as `CONFIG.SYS`, `AUTOEXEC.BAT`, and `*.INI`). These files still exist on a Windows 95 system, but only for compatibility reasons.

Through its layered file system architecture (Figure 27 on page 139), Windows 95 offers such features as long file names (up to 255 characters long) and a dynamic system cache for file and network I/O.

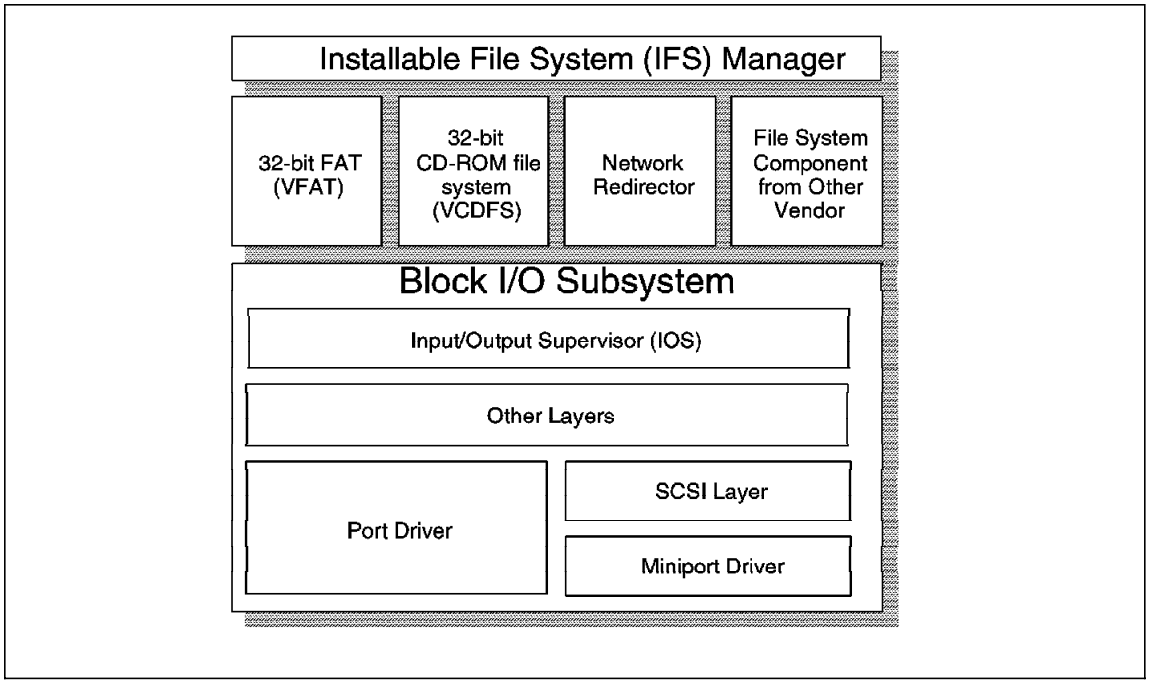


Figure 27. Windows 95 File System Architecture

The Windows 95 file system architecture is made up of the following components:

- The *Installable File System Manager* is responsible for arbitrating access to the different file system components.
- The *file system driver* layer includes access to the FAT-based disk devices, CD-ROM file systems, and redirected network device support.
- The *Block I/O Subsystem* is responsible for interacting with the physical disk device.

Windows 95 long file names are handled in the VFAT device driver. For each long file name on the system, an alias is recorded that falls within the 16-bit FAT 8.3 naming convention. It is this file name that is stored on the disk and used by any application that does not run through Windows 95.

8.2 Predisaster Preparation

The disaster we are preparing for is the total and catastrophic loss of the ADSM client, where provision has to be made to restore everything from the bare metal up. If this worst case scenario is covered by our disaster

recovery preparations, then we can assume that we will also be able to recover from lesser disasters.

In this section we discuss the kind of information that should be collected and saved before a disaster to enable a bare metal restore to take place when necessary.

To be prepared to recover from a disaster, collect and save the following information:

8.2.1 ADSM Backups

- For the methods used here we used the default include/exclude list that is installed by default for 32-bit Windows systems.
- Set the **Copy Serialization** parameter in the **Backup Copy Group** definition to *Shared Static*. This setting allows only those files not being modified to be included in the ADSM backup (preventing a ″fuzzy″ backup). When using this setting, it is best to schedule the ADSM backup during a period of low utilization of the ADSM client. Because this ADSM backup is oriented to provide an image of the workstation to be used in case of disaster, all applications and subsystems running on the machine should be closed before the backup, so that you have the fewest number of open files.

8.2.2 Operating Environment of the ADSM Client

In preparation for disaster recovery, we recommend that you collect and save the information listed below in addition to the ADSM backup data. Depending on your installation, you could save this information by using the DRM feature, or you could save it on hardcopy stored offsite. The way in which you save the information is not as important as ensuring that it is saved **somewhere** where it can be readily retrieved along with the client recovery media when a disaster occurs.

- **Hardware configuration**

  Include information about the adapters in the system and processor, for example.

- **Disk partitioning**

  Note the partition information about your disks, including the volume labels, since this is how ADSM identifies and interacts with the disks. You can view this information with the FDISK utility.

- **Communications details**

  For TCP/IP environments, store the IP addresses of the client machine and ADSM server, the default route, and domain name server along with

any adapter-specific settings. To gather this information look in the Networks section of the Windows 95 Control Panel.

Optional: Statistics for Postdisaster Recovery Verification

You may want to gather and save information that can be used after a disaster recovery test once the restore process is completed, to validate that all information has indeed been restored correctly. Each installation will have its own ideas about the best way to verify that the recovery is complete. Some possible sources of information for this type of verification are:

- Total amount of data on each disk and in each directory. Right-click on the disk or directory in Explorer and select **Properties**.

8.2.3 Preparing the System

In this section we discuss creating a bootable image for Windows 95 and explain how you can prepare the system for recovery by using the techniques we suggest.

8.2.3.1 Assumptions

These instructions apply to Windows 95 machines using a token-ring adapter and TCP/IP. **Modifications may be necessary for this technique to work in other environments using other network adapters and communication protocols**.

The instructions apply to the following products:

- **Windows 95**
- **ADSM Windows 32-bit Version 2, Release 1 client code**
- **Any ADSM server that uses TCP/IP**

A complete ADSM backup as we describe in 8.2, “Predisaster Preparation” on page 139 should be available at the ADSM server, and the restore should be done to a hardware configuration similar to that of the original ADSM backup/archive client machine.

8.2.3.2 Configuration Used to Test This Technique

We tested this technique, using the following configuration:

- IBM PC 360 with 32 MB of RAM
- 16 Mbps token-ring attachment
- 1.6 GB enhanced IDE hard drive

  - Primary partition of 512 MB containing Windows 95 (DRIVE-C)
  - Extended Partition of 512 MB containing data (DRIVE-D)
  - Approximately 500 MB of free space.
- Windows 95 with *Windows 95 Service Pack 1* installed
- ADSM/AIX Version 2, Release 1, Level 0.3 client code
- ADSM/AIX Version 2, Release 1, Level 9 server code

8.2.3.3 Long File Name Considerations

When bare metal restore planning for a Windows 95 operating system, you face a number of difficulties. Because of the way in which Windows 95 deals with its long file names, conventional backup and restore methods rely on the backup application being run from within the Windows 95 operating system. Thus you have to reinstall Windows 95 for the restore. Because in the majority of modern environments the most time-consuming part of any restore operation is the reconfiguration necessary to introduce a new machine into the network environment, we believed this was not an acceptable alternative.

The primary goal of the early part of disaster recovery using ADSM is to provide enough of a system to connect to the server and initiate a data restore. With most modern operating systems this is made possible by the use of some kind of bootable diskettes that put a minimal system into operation with just enough function to connect to a server and initiate data transfer. With Windows 95 a number of areas must be considered for this operation, and there is neither a well-documented utility nor documentation to guide the user. For a bootable diskette method to work for Windows 95, the diskettes have to contain a minimal operating system that is capable of both network connectivity and dealing with the long file names. If we refer back to Figure 26 on page 138, we can see that this minimal system would have to contain elements of each of the major components of the Windows 95 architecture.

Production of a minimal system is possible. With some informed guess work and trial and error testing, this system can then be placed on diskettes and stored offsite in case of disaster. Since this method is both time consuming and complicated, we looked at other methods.

Using two free utilities available from either the Windows 95 install CD-ROM or the Microsoft world wide web site (*http://www.microsoft.com*), you can remove all of the long file names from a system and make backups of all of the important configuration files. It then becomes possible to use more conventional methods of backing up a system image. Once the base image

is recovered, long file names are re-enabled and the standard ADSM 32bit client is used to recover the complete system quickly to the last incremental backup state.

The way in which you back up the base Windows 95 system depends on the resources you have available:

1. If you have a locally attached backup device, you can back up an image of the operating system to that device and then restore from there.
2. If you have an OS/2 system available on the network, you can use the CID peer recovery method covered in Chapter 6, “Recovery of OS/2 and Windows from an OS/2 CID Peer” on page 107.
3. If you have neither of these available, you can use bootable DOS diskettes as created in 7.2.3.3, “Step-by-Step Instructions” on page 130.

In essence, once you have taken an ADSM backup of the base Windows 95 system in the appropriate fashion, it is not important how you boot the system and recover the FAT files.

Note:

Before beginning any work with your Windows 95 system, you should always make sure that you have an updated copy of the Windows 95 Startup Disk. This may be produced by using Control Panel - Add/Remove Programs - Startup Disk.

8.2.4 Backing Up the System without Long File Names

The first stage in preparing the system for backup is ideally taken directly after first installation. This will reduce the amount of data stored in this first backup and therefore the amount of time taken to recover the backup.

Once the Windows 95 system has been installed and the Windows 32-bit ADSM client has been installed and configured, install the LFNBK from the /Admin/Apptools/Lfnback directory and the ERU utility from the /Other/Misc/Eru directory of the Windows 95 install CD-ROM.

Note:

The files can also be downloaded from:

http://www.microsoft.com/windows/download/lfnb.exe

http://www.microsoft.com/windows/download/eruzip.exe

The ERU utility makes a copy of your Windows 95 configuration, either all the files or specific ones to a specified location. If the backup is made to a file on your hard disk, this may then be backed up with ADSM and a pointer to it stored in DRM for postdisaster recovery. For the purposes of this test, we backed up all of the files to a diskette.

The LFNBK utility removes all long file names from the specified hard disk. The utility is a command-line-only utility that has a number of flags:

```
C: \disaster\LFNBACK\lfnbk -?
lfnbk: long file name backup/ restore utility Version 3.2
       (c)Copyright Microsoft Corp 1993-1995
usage: lfnbk (/v) (/b | /r | /pe) (/p) (c:)
       /v          verbose mode
       /b          backup and remove long filenames
       /pe         extract errors from backup database
       /r          restore backed up long file names
       /nt         do not restore backed up date and times
       /p          find long filenames but do not convert
       /force      force lfnbk to run even if not safe
```

If you are unsure about using this utility on your system, we recommend that you take a full ADSM incremental backup of the drive on which you intend to run the utility **before** you begin. You can then run the utility with the /p flag so that it will produce a list of all long file names on your system but not convert them. This list can then be checked for any possible causes of problems. The majority of the files required to operate Windows 95 are stored in shortened 8.3 format.

You can now produce the disaster recovery system image by following these steps:

1. Make a backup of your system config files, using the ERU utility.
2. Relabel the system drive. For example:

   ```
   C: \>LABEL
   Volume in drive C is DRIVE-C
   Volume Serial Number is 1227-15FC
   Volume label (11 characters, ENTER for none)? DRIVE-C1
   ```

   This allows ADSM to keep the backup without long file names and the standard daily incremental backups in separate file spaces on the server storage.
3. Open the Control Panel and select System - Performance, File Systems, and Troubleshooting and tick the Disable long name preservation for old programs.

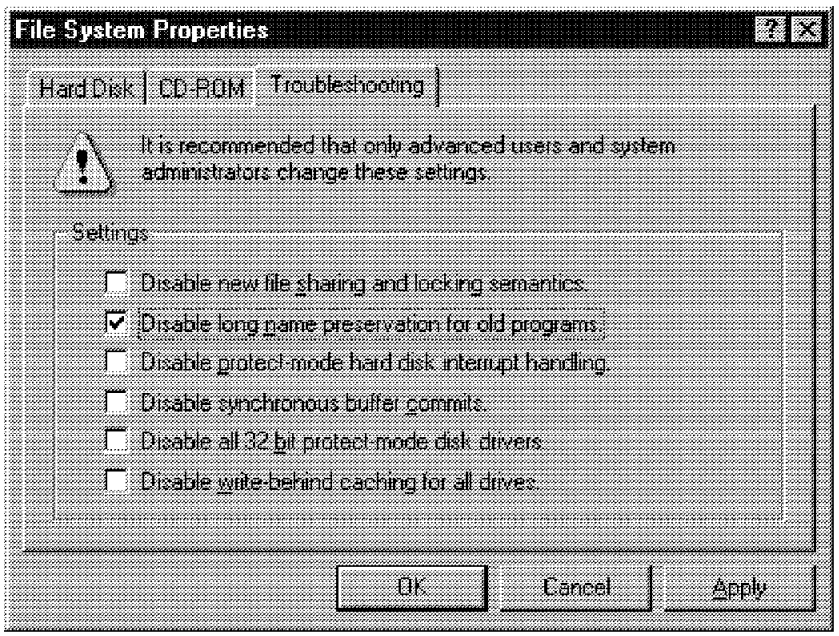


Figure 28. Disable Tunneling

This disables a process called *Tunneling*, which Windows 95 uses to conserve long file names when a file is used by a program that does not support the long file name protocol. Once you have clicked the Apply button, you will be asked to restart the computer.

4. Change to the directory containing the LFNBK utility and run the command with the /v /b flags. For example:

   ```
   C: \disaster\LFNBACK\> LFNBK /V /B C:
   ```

   This will show a long list of the file names being converted followed by output similar to the following:

   ```
   Dirs processed:                 235
   Files processed:                1832
   Lfns found:                     1279
   Lfns removed:                   1279
   ```

   This actually produces a file called LFNBK.DAT in the root of the drive being converted which contains information about the long file names and their shortened versions.

5. Next start the ADSM Windows 32-bit client by changing to the ADSM client directory (\ADSM32 by default) and using the command DSM. This

will start up the Backup-Archive client GUI from where you can take an incremental backup of your Windows 95 operating system.

6. Exit from the ADSM client interface and return to the LFNBK directory and execute this command:

   ```
   LFNBK /R
   ```

   to restore the long file names on your system.

7. Relabel the drive to its original name, reenable tunneling, and reboot your Windows 95 system.

This short file name system backup is now ready to be restored by one of the bootable methods that support the FAT file system. If you have a machine running OS/2 Warp in your environment, we would suggest following the steps in Chapter 6, “Recovery of OS/2 and Windows from an OS/2 CID Peer” on page 107 to build *CID Peer Recovery* diskettes. This method, once set up, is very easy to use. If you do not have such a machine available, you can use the method in 7.2.3.3, “Step-by-Step Instructions” on page 130 to create DOS bootable diskettes with the DOS ADSM client code included.

Once you have a bootable system, you can test that you can boot the system and make contact with the required machine, the ADSM server for the DOS diskettes, and a peer server for the OS/2 diskettes. You can then continue to make your daily ADSM backups of the client machine and wait for a disaster to happen.

Note: We used this method successfully on a variety of Windows 95 systems. As a result of publishing the draft book early on the world wide web, we received some reports that the **LFNBK /R** utility did not restore the 3.5-inch floppy disk drive file name correctly in some instances. As this book goes into hardcopy production, we are looking at some alternative utilities and will publish the results in subsequent editions. Any updates will appear first on the web version of the book—see http://www.redbooks.ibm.com and look under ″Redpieces.″

8.3 Postdisaster Recovery

In this section we describe how to recover from a disaster to the Windows 95 ADSM client environment using the information we saved before the disaster (described in 8.2, “Predisaster Preparation” on page 139).

To simulate a disaster we formatted the Windows 95 system drive and made sure that the system could no longer boot.

8.3.1 Rebuild Hardware Environment

Retrieve information about the Windows 95 machine to help re-create the hardware environment of the destroyed ADSM client. The new replacement machine must have a similar configuration.

If DRM had been used as the repository for this type of information, you can retrieve it by issuing the appropriate ADSM queries to the ADSM server. For examples of these queries, see 1.3.6, “Disaster Recovery Manager” on page 18.

8.3.2 Boot the Recovery System

Format the drive to which you are planning to restore the system to ensure that it is in FAT format and has the Windows 95 bootstrap on it. This may be done by booting from the Windows Startup Disk and then using:

```
a: \>FORMAT C: /S
```

to format the disk and place the bootstrap code in the disk’s boot sector. When prompted label the drive DRIVE-C.

Once this has been done you can recover the base system image from ADSM (in our example, the filespace labeled DRIVE-C1): Reboot the machine using the diskettes that match the method you have chosen to use. If you chose to use the OS/2 peer recovery technique, see 6.3.2, “Booting the Recovery System” on page 117 for the steps to recover the ADSM backup of your system.

If you used the DOS bootable diskette method, see 7.3.2, “Boot the Recovery System” on page 133 for the steps to recover the ADSM backup of your system.

You will now be able to boot into your Windows 95 system. The boot may fail once or even twice, but if it does, just reboot again and select Normal from the menu. Once the system is up, use Start - Run and type in:

```
C: \>\WINDOWS\DOSPRMPT
```

to call up a DOS window. In the DOS window, change to the LFNBK directory and run the utility with the /R flag. This will then restore all of the long file names to your system. You can then reenable tunneling as you did before and reboot the system.

Once the system has finished rebooting, you can relabel the drive and use the ADSM Windows 32-bit client interface to restore the rest of the files. The easiest way to do this is to make sure that there are no other applications

running and then do a full restore using the ADSM GUI. You may receive a warning indicating that the restore has failed on some files, but those files are just the files that are open and in use during the restore. See Figure 29 on page 148 for the options selection.

Note:

The files open and in use during the final restore usually will not have changed between backups. If, however, you apply something such as a Windows 95 Service Pack, it is important that you update the short file name backup image.

Figure 29. Windows 95 Full Restore

You may now reboot the system and continue normal operations.

8.3.2.1 Restoring a Drive

If the drive that has failed does not have the operating system on it, the procedure is simple:

1. Replace the drive.
2. Repartition if required.
3. Label partitions as they were before the disaster.
4. Restore from the ADSM backup, using the Windows 32-bit client.

8.3.2.2 Restoring a File

If files become damaged or deleted on the system, they may simply be restored by the user with the ADSM client interface.

8.3.2.3 Verify the Postdisaster Restoration

At this point, you would use any statistics you saved with your ADSM backups and bootable image to verify that they are comparable to those you receive after your recovery is complete.

8.3.3 Other Topics

Obviously the topics discussed here depend on certain software and/or hardware being available within your environment. As long as the bulk of the system is backed up with ADSM or another backup utility, you will always be able to recover the system by reinstalling the operating system. What we have tried to offer here are some alternatives that may seem at first to be more work than a reinstall but in the event of a disaster may be faster and able to be done by unskilled staff at a remote site.

This method may be further customized and refined by using one short file name backup as the disaster recovery for all of your Windows 95 systems. Because the method does not rely on the communications settings within the backup itself, a base image can be used to restore any machine in the environment. This machine then has to be reconfigured with its own IP address and other configuration details, but even so it is still much faster than reinstalling the whole operating system.

Chapter 9. Windows NT Version 3.51 Recovery

In this chapter we review the use of bootable diskettes and a recovery partition to recover a Windows NT Version 3.51 client environment that uses TCP/IP to communicate with its ADSM server.

We discuss the kind of information that should be backed up in preparation for a disaster, how to create the bootable diskettes and the recovery partition, and then how to make use of them in conjunction with a previous ADSM backup to recover a Windows NT Version 3.51 environment after a disaster.

Note: When we published the web version of this book, we included some specific examples of Windows NT V3.51 recovery. These are available on the Redbooks web pages at http://www.redbooks.ibm.com. They are being expanded and incorporated into a new Windows NT Recovery book.

9.1 Product Overview

Windows NT Version 3.51 is a multipurpose network operating system that offers high-performance file, print, and communications services. It supports both FAT and NTFS files.

The registry on Windows NT is a central database that contains information about hardware, applications, and operating system settings for each machine on the network. It also provides security and control over system, security, and account settings.

The Windows NT startup process involves two stages: a boot stage and a load stage. The boot stage involves reading the BOOT.INI file to see which NT partitions containing an operating system are available to be loaded. Because the load can be done only from a fixed disk, it is not possible to start up Windows NT entirely from diskettes. So recovering an inoperable production Windows NT partition requires one of the following:

- Reinstallation of Windows NT from scratch, using the system installation CD (or, depending on the disaster, the emergency repair diskette created during the original NT installation)

  or, to avoid having to reinstall Windows NT

- Having a diskette to initiate the startup process and a minimal version of Windows NT on a different partition on the same machine. This should preferably be a different physical hard drive and if possible a different hard disk controller from the production partition being protected so that the NT load can be completed from there.

In this chapter we focus on having a diskette to initiate the Windows NT startup process, which is completed by loading a minimal version of Windows NT from a different partition so that ADSM recovery using the Windows 32-bit ADSM client can be initiated.

9.2 Predisaster Preparation

The disaster we are preparing for is the total loss of the operating system disk of the ADSM client, where provision has to be made to restore everything from the bare metal up. If this worst case scenario is covered by our disaster recovery preparations, then we can assume that we will also be able to recover from lesser disasters.

In this section we discuss the kind of information that should be collected and saved before a disaster to enable a bare metal restore to take place when necessary.

To be prepared to recover from a disaster, collect and save the following information:

9.2.1 ADSM Backups

- The ADSM backup to be used in this restore technique should be done using the default DSM.OPT of the ADSM Windows 32-bit client.
- The ADSM backup should include a copy of the registry. (By default the ADSM 32-bit Windows client will back up the entire registry when an incremental backup is performed on the system partition.)
- We also recommend that you use the shared static option within the backup copy group to avoid ″fuzzy″ backups.

9.2.2 Operating Environment of the ADSM Client

In addition to the files backed up by the ADSM client, we recommend that you collect and save the information listed below before a disaster. Depending on your installation, you could save this information by using the DRM feature, or you could save it on hardcopy stored offsite. The way in which you save the information is not as important as ensuring that it is saved **somewhere** where it can be readily retrieved along with the client recovery media when a disaster occurs.

- **Hardware configuration**

  Record the partition information for the primary hard disk.

- **Communications details**

  Although this method is not protocol specific, it is considered sound practice to keep details about the network configuration such as the IP address and host name.

Optional: Statistics for Postdisaster Recovery Verification

You may want to gather and save information that can be used in a disaster recovery test once the restore process is completed, to validate that all information has been restored correctly. Each installation would have its own ideas about the best way to verify that the recovery is complete. Some possible sources of information for verification are:

- Total amount of data on the drive. Select each drive with the right mouse button and then select **properties**.
- Total amount of data in the directory. Select a directory with the right mouse button and then select **properties**.
- File associations and environment information. This may be found in **Control Panel, System** folder, **Environment** tab.

9.2.3 Creating the Bootable Diskettes and Recovery Partition

In this section we describe a method to create bootable diskettes and a recovery partition for Windows NT Version 3.51.

9.2.3.1 Assumptions

These instructions were tested on a Windows NT Version 3.51 machine using a token-ring adapter and TCP/IP. **Modifications may be necessary for this technique to work in other environments using other network adapters and communication protocols.** This technique should be valid, however, for all combinations of hardware and software that Windows NT Version 3.51 supports.

The instructions apply to the following products:

- **Windows NT Version 3.51**
- **ADSM Windows 32-bit Version 2, Release 1 client code**
- **Any ADSM server that uses TCP/IP**

A complete ADSM backup as we describe in 9.2, “Predisaster Preparation” on page 152 should be available at the ADSM server, and the restore should be done to a hardware configuration similar to that of the original ADSM backup/archive client machine.

9.2.3.2 Configuration Used to Test This Technique

We tested this technique, using the following configuration:

- IBM PC 360 with 32 MB of RAM
- 16 Mbps token-ring attachment
- 1.6 GB Enhanced IDE hard drive
- Partition information:
  - Primary partition of 512 MB containing Windows NT Version 3.51 (C:).
  - Logical drive of 500 MB containing Windows NT Version 4.0
  - Logical drive of 124 MB containing Windows NT Version 4 Recovery System
- ADSM Windows 32-bit Version 2, Release 1, Level 3 client code
- ADSM/AIX Version 2, Release 1, Level 9 server code

To use this technique you will need:

- One 1.44 MB diskette
- A copy of the Windows NT installation media
- Approximately 100 MB of free disk space (preferably unpartitioned)

9.2.3.3 Step-by-Step Instructions

Step 1: Install Minimal NT Configuration on Recovery Partition: Install the minimal Windows NT configuration on an alternative recovery partition, preferably a partition on a different physical drive and, if possible, a different hard disk controller from the production partition being protected against a disaster. Include TCP/IP, and add the ADSM 32-bit Windows client code. This recovery system must be the most recent version of Windows NT. For example, if you have Windows NT Version 3.51 and Windows NT Version 4.0 installed on the same system, the recovery system must be Windows NT Version 4.0. A Windows NT Version 3.51 NTLDR file cannot be used to load a Windows NT Version 4.0 system:

Edit the BOOT.INI file and change the partition description to something like ″Disaster Recovery NT 3.51 Partition.″ To edit the BOOT.INI file you must first change its attributes:

```
C:\> ATTRIB -S -R BOOT.INI
```

Once you have finished editing BOOT.INI remember to change the attributes back to system read-only; use the following command:

```
C:\> ATTRIB +S +R BOOT.INI
```

Step 2: Create Bootable Diskette Version of Windows NT Boot Manager: To provide a recovery alternative in case the NT system files on the C: drive are damaged:

- Format a 1.44 MB diskette.
- Copy the BOOTSEC.DOS, BOOT.INI, NTLDR, and NTDETECT.COM files from the C: drive of the machine to the diskette. To do the copy, first change the attributes of these files thus:

```
C:\> ATTRIB -S -H    BOOTSEC.DOS
C:\> ATTRIB -S -R    BOOT.INI
C:\> ATTRIB -S -H -R NTLDR
C:\> ATTRIB -S -H -R NTDETECT.COM
```

  Then copy the files to the diskette (make sure that BOOTSEC.DOS is the first file copied):

```
C:\> COPY C:\BOOTSEC.DOS  A:\BOOTSEC.DOS
C:\> COPY C:\BOOT.INI     A:\BOOT.INI
C:\> COPY C:\NTDETECT.COM A:\NTDETECT.COM
C:\> COPY C:\NTLDR        A:\NTLDR
```

  Change the attributes back to system read-only:

```
C:\> ATTRIB +S +H    BOOTSEC.DOS
C:\> ATTRIB +S +R    BOOT.INI
C:\> ATTRIB +S +H +R NTLDR
C:\> ATTRIB +S +H +R NTDETECT.COM
```

  Change the attributes back to system read-only on the diskette:

```
C:\> ATTRIB +S +H    A:\BOOTSEC.DOS
C:\> ATTRIB +S +R    A:\BOOT.INI
C:\> ATTRIB +S +H +R A:\NTLDR
C:\> ATTRIB +S +H +R A:\NTDETECT.COM
```

9.3 Postdisaster Recovery

In this section we describe how to recover from a disaster to the Windows NT Version 3.51 ADSM client environment using the information we saved before the disaster (described in 9.2, “Predisaster Preparation” on page 152), the boot diskettes and recovery partition we created (described in 9.2.3, “Creating the Bootable Diskettes and Recovery Partition” on page 153).

To simulate a disaster we formatted the C: partition containing all of the Windows NT Version 3.51 system files so that it would no longer boot.

9.3.1 Rebuild Hardware Environment

Retrieve information about the Windows NT Version 3.51 machine to help re-create the hardware environment of the destroyed ADSM client. The new replacement machine must have a similar configuration.

If DRM had been used as the repository for this type of information, you can retrieve it by issuing the appropriate ADSM queries to the ADSM server. For examples of these queries, see 1.3.6, “Disaster Recovery Manager” on page 18.

9.3.2 Start the Recovery System

The recovery system comprises the bootable diskette and recovery partition.

Recover the production partition by doing the following:

- Boot with the diskette boot manager.
- Start the ″recovery″ partition that was prepared before the disaster by using the cursor keys to select from the menu.
- Use the Windows NT disk administrator to partition the primary disk, using the information saved before the disaster.
- Reformat the primary C: drive as FAT or NTFS. Copy the system files from the boot manager diskette you created before the disaster to the C: drive. Remember to adjust the attributes before and after the copy as described in 9.2.3.3, “Step-by-Step Instructions” on page 154, and to copy the file called BOOTSECT.DOS first!

9.3.3 Restore from the ADSM Backup

You may now restore the whole system, a drive, or a file and, if you are testing your procedures, verify your recovery actions.

9.3.3.1 Restoring the Whole System

Now that the hardware is recovered and a minimal Windows NT server system is started up, you can invoke the ADSM client to begin ADSM recovery from the ADSM server:

- Use ADSM to restore all damaged partitions (using the original ADSM client options file that had been used on that machine to do the original ADSM backup).
- Use ADSM to restore the registry files.

  If we call the NT machine being restored NTBENJAMIN, and ADMINMEG is the name of the account that performed the ADSM backups, we would restore the production partition registry with the following ADSM commands:

```
DSMC RES C:/ADSM.SYS/REGISTRY/NTBENJAMIN/MACHINE/*.*
         C:/WINNT/SYSTEM32/CONFIG/

DSMC RES C:/ADSM.SYS/REGISTRY/NTBENJAMIN/USERS/DEFAULT
         C:/WINNT/SYSTEM32/CONFIG/

DSMC RES C:/ADSM.SYS/REGISTRY/NTBENJAMIN/USERS/ADMINMEG/*.*
         C:/WINNT/SYSTEM32/CONFIG/
```

- Reboot the machine and select the production system. The production partition should start and be in the same state it was in after the last ADSM backup. If the machine is a domain controller, it should be resynchronized with the primary domain controller.

9.3.3.2 Restoring a Drive or File

Files and drives other than the system drive can be restored with the ADSM client as usual.

9.3.3.3 Verify the Postdisaster Restoration

At this point, if this is part of a disaster test, you would use any statistics you saved with your ADSM backups and bootable image to verify that they are comparable to those you receive after your recovery is complete.

Chapter 10. Windows NT Version 4.0 Recovery

In this chapter we review the use of bootable diskettes and a recovery partition to recover a Windows NT Version 4.0 client environment that uses TCP/IP to communicate with its ADSM server.

We discuss the kind of information that should be backed up in preparation for a disaster, how to create the bootable diskettes and the recovery partition, and then how to make use of them in conjunction with a previous ADSM backup to recover a Windows NT Version 4.0 environment after a disaster.

10.1 Product Overview

Windows NT Version 4.0 is a multipurpose network operating system that offers high-performance file, print, and communications services. It supports both FAT and NTFS files.

The registry on Windows NT is a central database that contains information about hardware, applications, and operating system settings for each machine on the network. It also provides security and control over system, security, and account settings.

The Windows NT startup process involves two stages: a boot stage and a load stage. The boot stage involves reading the BOOT.INI file to see which NT partitions containing an operating system are available to be loaded. Because the load can be done only from a fixed disk, it is not possible to start up Windows NT entirely from diskettes. So recovering an inoperable production Windows NT partition requires one of the following:

- Reinstallation of Windows NT from scratch, using the system installation CD (or, depending on the disaster, the emergency repair diskette created during the original NT installation)

  or, to avoid having to reinstall Windows NT

- Having a diskette to initiate the startup process and a minimal version of Windows NT on a different partition on the same machine (preferably a different physical hard drive and if possible a different hard disk controller from the production partition being protected) so that the NT load can be completed from there

In this chapter we focus on having a diskette to initiate the Windows NT startup process, which is completed by loading a minimal version of

Windows NT from a different partition so that ADSM recovery using the Windows 32-bit ADSM client can be initiated.

10.2 Predisaster Preparation

The disaster we are preparing for is the total loss of the operating system disk of the ADSM client, where provision has to be made to restore everything from the bare metal up. If this worst case scenario is covered by our disaster recovery preparations, then we can assume that we will also be able to recover from lesser disasters.

In this section we discuss the kind of information that should be collected and saved before a disaster to enable a bare metal restore to take place when necessary.

To be prepared to recover from a disaster, collect and save the following information:

10.2.1 ADSM Backups

- The ADSM backup to be used in this restore technique should be done using the default DSM.OPT of the ADSM Windows 32-bit client.
- The ADSM backup should include a copy of the registry. (By default the ADSM 32-bit Windows client will back up the entire registry when an incremental backup is performed on the system partition.)
- We also recommend that you use the shared static option within the backup copy group to avoid ″fuzzy″ backups.

10.2.2 Operating Environment of the ADSM Client

In addition to the files backed up by the ADSM client, we recommend that you collect and save the information listed below before a disaster. Depending on your installation, you could save this information by using the DRM feature, or you could save it on hardcopy stored offsite. The way in which you save the information is not as important as ensuring that it is saved **somewhere** where it can be readily retrieved along with the client recovery media when a disaster occurs.

- **Hardware configuration**

  It is important to maintain the current partition information for the disks in the system and the labels that have been assigned to them. This information can be obtained from the Windows NT Disk Administrator utility.

- **Communications details**

  Although this method is not protocol specific, it is considered sound practice to keep details about the network configuration (for example, the IP address and HostName). This information is found in the **protocol-properties** section of **Networks** in the **Control Panel**.

Optional: Statistics for Postdisaster Recovery Verification

You may want to gather and save information that can be used post-disaster once the restore process is completed, to validate that all information has indeed been restored correctly. Each installation would have its own ideas about the best way to verify that the recovery is complete. Some possible sources of information for verification are:

- Total amount of data on the drive. Select each drive with the right mouse button and then select **properties**.
- Total amount of data in the directory. Select a directory with the right mouse button and then select **properties**.
- File associations and environment information may be found in **Control Panel, System** folder, **Environment** tab.

10.2.3 Creating the Bootable Diskettes and Recovery Partition

In this section we describe a method to create bootable diskettes and a recovery partition for Windows NT Server Version 4.0.

10.2.3.1 Assumptions

These instructions were tested on a Windows NT Version 4.0 machine using a token-ring adapter and TCP/IP. **Modifications may be necessary for this technique to work in other environments using other network adapters and communication protocols**, but this technique should be valid for all combinations of hardware and software that Windows NT Version 4.0 supports.

The instructions apply to the following products:

- **Windows NT Version 4.0**
- **ADSM Windows 32-bit Version 2, Release 1 client code**
- **Any ADSM server that uses TCP/IP**

A complete ADSM backup as we describe in 10.2, “Predisaster Preparation” on page 160 should be available at the ADSM server, and the restore should be done to a hardware configuration similar to that of the original ADSM backup/archive client machine.

10.2.3.2 Configuration Used to Test This Technique

We tested this technique, using the following configuration:

- IBM PC 360 with 32 MB of RAM
- 16 Mbps token-ring attachment
- 1.6 GB Enhanced IDE hard drive
- Partition information:
  - Primary partition of 512 MB containing Windows NT Version 4.0 (C:).
  - Logical drive of 500 MB containing Windows NT Version 3.51
  - Logical drive of 124 MB containing Windows NT Version 4.0 Recovery System
- ADSM Windows 32-bit Version 2, Release 1, Level 3 client code
- ADSM/AIX Version 2, Release 1, Level 9 server code

To use this technique you will need:

- One 1.44 MB diskette
- A copy of the Windows NT installation media
- Approximately 100 MB of free disk space (preferably unpartitioned)

10.2.3.3 Step-by-Step Instructions

Step 1: Install Minimal NT Configuration on Recovery Partition: Install the minimal Windows NT Server configuration on an alternative recovery partition, preferably a partition on a different physical drive and, if possible, a different hard disk controller. Include TCP/IP, and add the ADSM 32-bit Windows client code. This recovery system must be the most recent version of Windows NT. For example, if you have Windows NT Version 3.51 and Windows NT Version 4.0 installed on the same system, the recovery system must be Windows NT Version 4.0. A Windows NT Version 3.51 NTLDR file cannot be used to load a Windows NT Version 4.0 system. Edit the BOOT.INI file and change the partition description to something like ″Disaster Recovery NT 4.0 Partition.″

```
(boot loader)
timeout=30
default=multi(0)disk(0)rdisk(0)partition(3)\WINNT
(Operating Systems)
multi(0)disk(0)rdisk(0)partition(3)\WINNT="NT Recovery System 4.00"
multi(0)disk(0)rdisk(0)partition(3)\WINNT="NT Recovery System 4.00 (VGA
                                                mode)"/basevideo /sos
multi(0)disk(0)rdisk(0)partition(2)\WINNT="Windows NT Server 4.00"
multi(0)disk(0)rdisk(0)partition(1)\WINNT35="Windows NT Server 3.51"
multi(0)disk(0)rdisk(0)partition(1)\WINNT35="Windows NT Server 3.51"
```

To edit the BOOT.INI file you must first change its attributes, using the following command:

```
C:\> ATTRIB -S -R BOOT.INI
```

Once you have finished editing BOOT.INI remember to change the attributes back to system read-only; use the following command:

```
C:\> ATTRIB +S +R BOOT.INI
```

Step 2: Create Bootable Diskette Version of Windows NT Boot Manager: To provide a recovery alternative in case the NT system files on the C: drive are damaged:

- Format a 1.44 MB diskette using Windows NT (any version).
- Copy the BOOTSEC.DOS, BOOT.INI, NTLDR, and NTDETECT.COM files from the C: drive of the machine to the diskette. Use the Windows NT Explorer if the **Show All Files** is selected and the **Hide extensions for all known file types** option is deselected. To do the copy from a command line prompt, first change the attributes of these files thus:

  ```
  C:\> ATTRIB -S -H    BOOTSEC.DOS
  C:\> ATTRIB -S -R    BOOT.INI
  C:\> ATTRIB -S -H -R NTLDR
  C:\> ATTRIB -S -H -R NTDETECT.COM
  ```

  Then copy the files to the diskette (make sure that BOOTSEC.DOS is the first file copied):

  ```
  C:\> COPY C:\BOOTSEC.DOS  A:\BOOTSEC.DOS
  C:\> COPY C:\BOOT.INI     A:\BOOT.INI
  C:\> COPY C:\NTDETECT.COM A:\NTDETECT.COM
  C:\> COPY C:\NTLDR        A:\NTLDR
  ```

  Change the attributes back to system read-only:

  ```
  C:\> ATTRIB +S +H    BOOTSEC.DOS
  C:\> ATTRIB +S +R    BOOT.INI
  C:\> ATTRIB +S +H +R NTLDR
  C:\> ATTRIB +S +H +R NTDETECT.COM
  ```

Change the attributes back to system read-only on the diskette:

```
C:\> ATTRIB +S +H    A:\BOOTSEC.DOS
C:\> ATTRIB +S +R    A:\BOOT.INI
C:\> ATTRIB +S +H +R A:\NTLDR
C:\> ATTRIB +S +H +R A:\NTDETECT.COM
```

Note:

If the attributes are not returned to their default settings, neither the machine nor the diskette will boot.

10.3 Postdisaster Recovery

In this section we describe how to recover from a disaster to the Windows NT Version 4.0 ADSM client environment using the information we saved before the disaster (described in 10.2, “Predisaster Preparation” on page 160), the boot diskettes and recovery partition we created (described in 10.2.3, “Creating the Bootable Diskettes and Recovery Partition” on page 161).

To simulate a disaster, we formatted the C: partition containing all of the Windows NT Version 4.0 system files so that it would no longer boot.

10.3.1 Rebuild Hardware Environment

Retrieve information about the Windows NT Version 4.0 machine to help re-create the hardware environment of the destroyed ADSM client. The new replacement machine must have a similar configuration.

If DRM had been used as the repository for this type of information, you can retrieve it by issuing the appropriate ADSM queries to the ADSM server. For examples of these queries, see 1.3.6, “Disaster Recovery Manager” on page 18.

10.3.2 Start the Recovery System

The recovery system comprises the bootable diskette and recovery partition.

Recover the production partition by doing the following:

- Boot with the diskette boot manager:

```
OS Loader V4.00

Please select the operating system to start

     NT Recovery System 4.00
     NT Recovery System 4.00 ·VGA mode“
     Windows NT Server Version 4.00
     Windows NT Server Version 4.00 ·VGA mode“
     Windows NT Server Version 3.51
     Windows NT Server Version 3.51 ·VGA mode“
     Microsoft Windows 95


Please use cursor up and cursor down to highlight your choice.
Press Enter to select.
```

- Start the ″recovery″ partition that was prepared before the disaster by using the cursor keys to select from the menu.
- Use the Windows NT disk administrator to partition the primary disk, using the information saved before the disaster.
- Reformat the primary C: drive as FAT or NTFS. Copy the system files from the boot manager diskette you created before the disaster to the C: drive. Remember to adjust the attributes before and after the copy as described in 10.2.3.3, “Step-by-Step Instructions” on page 162, and to copy the file called BOOTSECT.DOS first!

10.3.3 Restore from the ADSM Backup

10.3.3.1 Restoring the Whole System

Now that the hardware is recovered and a minimal Windows NT Server system is started up, you can invoke the ADSM client to begin ADSM recovery from the ADSM server:

- Use ADSM to restore all damaged partitions (using the original ADSM client options file that had been used on that machine to do the original ADSM backup).

Note:

Remember you will need to access the ADSM server with the node name of the machine you are recovering, for example this may be done from the command line by using:

```
C: DSMC -NODENAME=BENJAMIN
```

- Next, use ADSM to restore the registry files.

  If we call the NT machine being restored BENJAMIN with a single administrator of name MEGAN, we would restore the production partition registry with the following ADSM commands:

```
DSMC RES C:/ADSM.SYS/REGISTRY/BENJAMIN/MACHINE/*.*
         C:/WINNT/SYSTEM32/CONFIG/

DSMC RES C:/ADSM.SYS/REGISTRY/BENJAMIN/USERS/DEFAULT
         C:/WINNT/SYSTEM32/CONFIG/

DSMC RES C:/ADSM.SYS/REGISTRY/BENJAMIN/USERS/MEGAN/*.*
         C:/WINNT/SYSTEM32/CONFIG/
```

- Reboot the machine and select the production system. The production partition should start and be in the same state it was in after the last ADSM backup. If the machine is a domain controller it should be resynchronized with the primary domain controller.

10.3.3.2 Restoring a Drive or File

Files and drives other than the system drive can be restored with the ADSM client as usual.

10.3.3.3 Verify the Postdisaster Restoration

At this point, you would use any statistics you saved with your ADSM backups and bootable image to verify that they are comparable to those you receive after your recovery is complete.

Chapter 11. Novell NetWare Version 3.12 Recovery

In this chapter we discuss some techniques to recover a Novell NetWare Version 3.12 server environment by using bootable diskette recovery.

We examine the minimum resources and information required to build a base Novell NetWare Version 3.12 system that is capable of running an ADSM client using a TCP/IP connection to the ADSM server. We document the steps to create bootable diskettes and then walk through the recovery of a Novell NetWare Version 3.12 server using these bootable diskettes to enable ADSM recovery to begin on the re-created Novell NetWare environment using TCP/IP (see Figure 30 on page 168).

We also discuss the bare metal restore of Novell NetWare Version 3.12 servers that use the bootable diskettes, but in conjunction with a peer Novell NetWare server which is used to do the ADSM recovery. This is an alternative method for those Novell NetWare ADSM clients that do not use TCP/IP to communicate with their ADSM server (perhaps they have NetWare for SAA installed and use SNA APPC instead). In this case, because the bootable diskette technique covers TCP/IP communications only, we rely on a peer Novell NetWare server that is still a functioning ADSM client to do the ADSM restore on behalf of the Novell NetWare server being recovered. Once the peer Novell NetWare server has finished restoring files from ADSM, communications between the ADSM server and the restored Novell NetWare ADSM client can be reestablished.

Note: The techniques described here do not include recovery of any files or programs you stored on the DOS partition. If you do have the need to recover this DOS partition, you can refer to the technique described in Chapter 7, “DOS/Windows Version 3.1 Recovery” on page 125.

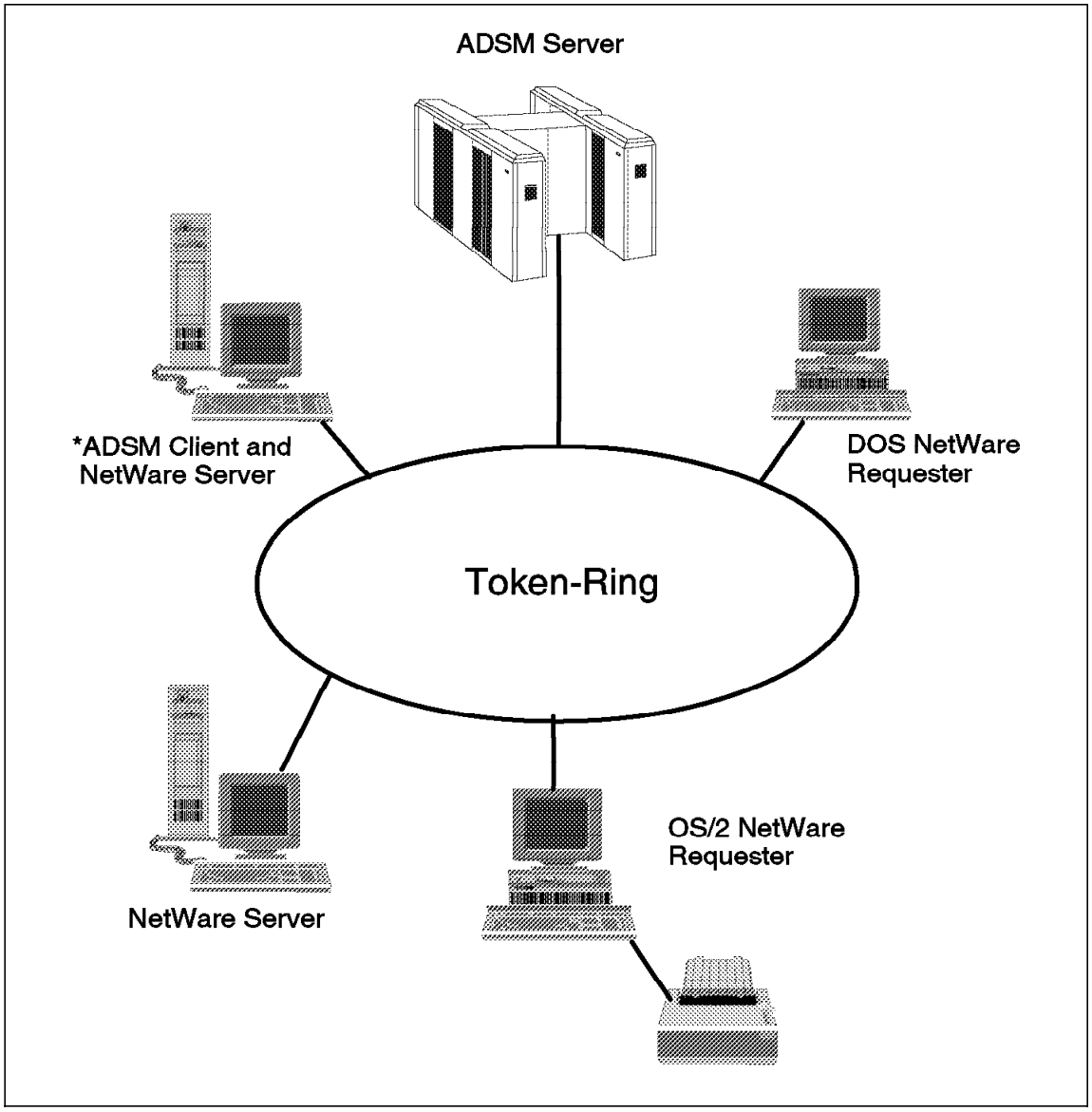


Figure 30. Recovering the NetWare Version 3.12 Server and ADSM Client

11.1 Product Overview

Novell NetWare Version 3.12 is a multitasking network operating system (NOS). It is, however, not considered a native operating system, as by itself it is not bootable. It needs DOS to load its base kernel, SERVER.EXE. (For a detailed description of the architecture of the operating system, refer to the

Novell NetWare 3.12 publications or the Novell homepage at http://www.novell.com.)

After SERVER.EXE is loaded, it takes over the control and continues the start up process. It locates and executes the STARTUP.NCF file. The most important statement in this NetWare command file (NCF) is the statement to load the required disk driver. This statement enables NetWare to mount and access its volumes, particularly the SYS volume where the NetWare loadable modules (NLMs) reside. Required NLMs are loaded to build up the NOS.

The next NCF that SERVER.EXE fetchs and executes is the AUTOEXEC.NCF, normally found in the SYS:/SYSTEM directory. Typically, AUTOEXEC.NCF includes statements to load other disk drivers, LAN drivers, and Novell NetWare utilities and applications.

11.1.1 File System

In the NetWare file system, the physical disk is not explicitly addressable as in the case of DOS and OS/2 operating systems. The NetWare file system includes the definitions of partition and volume and the concepts of directory, subdirectory, file, and bindery.

11.1.1.1 Partition

The free space on a physical disk must be partitioned as a NetWare partition before NetWare volumes can be defined. Only one NetWare partition can be defined per physical disk.

11.1.1.2 Volume

A NetWare volume can occupy part or all of the disk space of a NetWare partition. A NetWare volume can also span multiple NetWare partitions.

To operate, NetWare needs the minimum, a SYS volume. By default, NetWare assigns all disk space on its first partition as SYS. The size may be redefined during the installation process.

A volume in NetWare is equivalent to a physical or logical drive (for example, C: or E:) in DOS or OS/2.

11.1.1.3 Directory and File

The concept of directory, subdirectory, and file in NetWare is the same as in the DOS and OS/2 operating systems. However, a volume name instead of a drive letter is used when specifying a path. NetWare, as a network file system, also allows file access across different servers. To identify a file on a different server, the server name must be included in the path. A fully qualified path definition takes the following form:

SERVER_NAME/VOLUME_NAME:DIRECTORY_NAME/SUB-DIRECTORY_NAME/FILE_NAME

Note: In NetWare, slash (/) and backslash (\) are interchangeable when specifying a directory or subdirectory.

11.1.1.4 Bindery

NetWare Version 3.12 controls access to its system resources by maintaining an access and security database known as the *bindery*. The bindery consists of three hidden files, located on the SYS:SYSTEM directory: NET$OBJ.SYS, NET$PROP.SYS, and NET$VAL.SYS. These three files contain the object definitions, object properties, and values of the object definitions, respectively.

11.1.2 Storage Management Services

Storage management services (SMS) of Novell NetWare Version 3.12 provide a well-defined API for managing NetWare′s bindery and file system. This API ensures consistency across different versions of the NetWare operating system. Hence, vendors′ storage management applications can be written to be version independent.

11.1.2.1 Storage Management Engine

The storage management engine (SME) is the general term used for a storage management application that runs on the NetWare server; that is, an application that has been written to the NetWare SMS API. The ADSM NetWare backup/archive client is an SME.

11.1.2.2 Storage Management Data Requester

SME does not communicate with the NetWare server directly. The storage management data requester (SMDR) does. SMDR, an NLM provided by the SME, basically acts as a communication vehicle for SMS. It conveys requests between SME and the target service agent (TSA). It also provides communication paths between SMDRs. SMDR allows movement of data between NetWare servers; it does not perform physical data movement.

11.1.2.3 Target Service Agent

TSA, an NLM provided by the application, acts on requests from the SME. TSA adheres to the NetWare file system architecture requirement and performs the data movement accordingly. Figure 31 on page 171 shows the interrelationships of these elements.

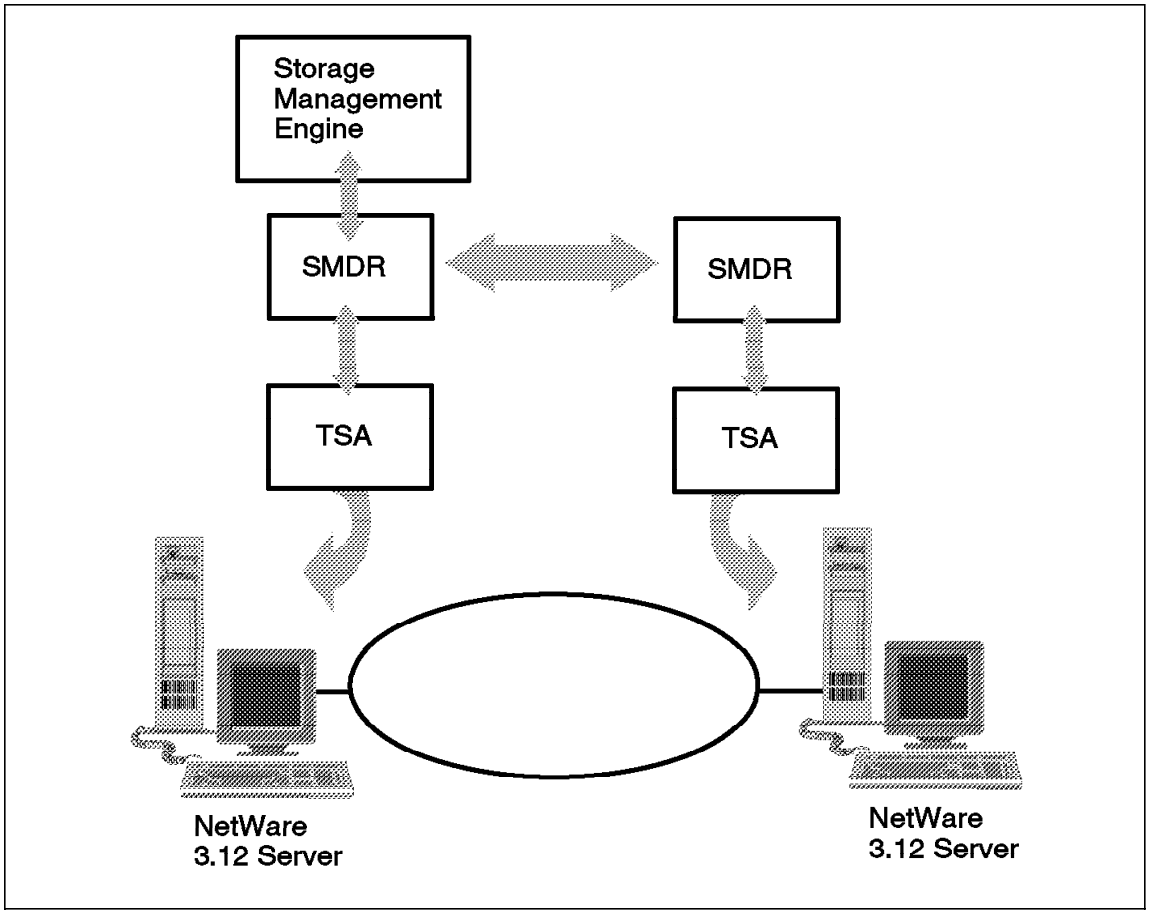


Figure 31. Novell NetWare SMS Components

11.1.3 Communication Protocols

Novell NetWare servers use the Internetwork Packet Exchange/ Sequenced Packet Exchange (IPX/SPX) protocol to communicate with each other as well as with any requester on the server. NetWare servers also include part of TCP/IP in their base, thus enabling them to communicate with other systems that do not support the IPX/SPX protocol (for example, VM and MVS operating systems).

Novell NetWare does not support SNA. However, a separate licensed product, NetWare for SAA, is available to provide SNA connectivity for the Novell NetWare server.

11.2 Predisaster Preparation: Bootable Diskettes

The disaster we are preparing for is the total and catastrophic loss of the ADSM client, where provision has to be made to restore everything from the bare metal up. If our disaster recovery preparations can cover this worst case scenario, we can assume that they will also be able to handle recovery from lesser disasters.

In this section we discuss the information to collect and save before a disaster to enable a bare metal restore.

11.2.1 ADSM Backups

We recommend that you include the bindery and all volumes (including the volume restrictions and trustee directory assignments) in the ADSM backup that will eventually be used for the ADSM restore part of the bare metal recovery of the Novell NetWare server platform.

For more information about ADSM backups, have a look at *Getting Started with ADSM NetWare Clients*, GG24-4242.

11.2.2 Operating Environment of the ADSM Client

In preparation for disaster recovery we recommend that you collect and save offsite the information listed below in addition to the ADSM backup data. Depending on your installation, you could save this information by using the DRM feature, or you could save it on hardcopy stored offsite. The way in which you save the information is not as important as ensuring that it is saved **somewhere** where it can be easily retrieved along with the client recovery media when a disaster occurs.

- **Software Configuration**

  Save information about the version of DOS you are using. To check the DOS version currently installed on the NetWare server, bring down the server (use the DOWN command from the server console) and exit to DOS (use the EXIT command). It is not necessary to use the same level or vendor of DOS as on the working server to build the bootable diskettes. If a different DOS version is used, however, that version will be the DOS version for the newly recovered server.

  Record whether boot manager is installed on the C: drive. DOS does not support the management of the boot manager partition. If the boot manager partition is mandatory for the machine, you will need (bootable) diskettes from other operating systems (for example, OS/2) or vendor products that provide this utility, as well as the documentation explaining its use.

- **Hardware Configuration**

Record the size of the C: drive. You have to bring down the server to be able to check the capacity of the C: drive with FDISK or CHKDSK. Depending on how the NetWare system was originally installed, you may need a slightly bigger C: drive to house all files from the bootable diskettes. A size of 5 MB is ideal.

If a specific disk driver is required for DOS to access the drive, note it. You can check this from the CONFIG.SYS file. Be aware that you may not be using the same type of disk in your recovery hardware.

Use the NetWare install utility, INSTALL.NLM, to collect the following information:

- Number of partitions in the server and their respective sizes
- Capacity of the SYS volume
- Block size used for the SYS volume
- Similar information for any other volumes on the server

Record all disk and LAN drivers used. You can get this information from the STARTUP.NCF and AUTOEXEC.NCF files. During the actual recovery, you may not always be able to use the exact same make of hardware. If different types of disk or LAN drivers are used for the new replacement machine, the required drivers for both DOS and NetWare must be available.

If a name space other than DOS is used, record this information also. Use the VOLUMES console command to list the name space added to each of the volumes.

- **Communications Details**

  Record the NetWare server's name, the IPX internal network number, its TCP/IP address, as well as the gateway TCP/IP address used by this server. This information is recorded in AUTOEXEC.NCF. You can also get the same information from the server console by issuing the CONFIG command. To get this network information from the server console, the corresponding network has to be started first.

  The TCP/IP information for the ADSM client will be required only at later stages of the server recovery when files from the bootable diskettes can be accessed and copied. So this information can be precoded in an NCF (we used TCPRECOV.NCF) and run from the server console.

  Record the ADSM server's TCP/IP address and TCP port address, as well as the ADSM client node name. This information can be found in the client options file (DSM.OPT) in the SYS:/ADSM directory.

  Note: Depending on your installation, you can also record the password associated with the ADSM client node name. You may prefer, for

reasons of security, to simply reset all ADSM client passwords if you cannot remember them.

11.2.3 Creating the Bootable Diskettes

In this section we describe a technique for creating bootable diskettes for Novell NetWare Version 3.12. After a disaster, you use these diskettes to quickly boot a replacement machine with the minimal operating system, communications, and ADSM software necessary to begin file restoration with the ADSM client and server. Normal ADSM recovery can then be used to recover the remainder of the predisaster client environment.

11.2.3.1 Assumptions

These instructions apply to machines running Novell NetWare Version 3.12, using a token-ring adapter and TCP/IP for communications between the NetWare ADSM client and the ADSM server. *Modifications may be necessary for this technique to work in environments using other network adapters, hard disk controllers, and so on.*

The instructions apply to the following products:

- *Novell NetWare Version 3.12*
- *Any ADSM server that uses TCP/IP*

A complete ADSM backup as described in 11.2, “Predisaster Preparation: Bootable Diskettes” on page 172 should be available at the ADSM server, and the restore should be done to a hardware configuration similar to that of the original ADSM backup/archive client machine.

11.2.3.2 Configuration Used to Test This Technique

We tested this technique, using the following configuration:

- PS/2 Model 95 with 32 MB of RAM
- 16 Mbps token-ring attachment
- One 400 MB hard drive, partitioned with a 5 MB DOS partition, with the rest of free space for the NetWare partition
- Novell NetWare Version 3.12
- ADSM NetWare Version 2, Release 1 client code
- ADSM/AIX Version 2, Release 1, Level 0.2 server code

11.2.3.3 Step-by-Step Instructions

These instructions for creating a set of Novell NetWare Version 3.12, TCP/IP, ADSM NetWare client enabled bootable diskettes are based on the method provided by Jerry Lawson of ITT Hartford.

To rebuild a Novell NetWare Version 3.12 system from bare metal that is capable of restoring backup data from the ADSM server through a TCP/IP connection, you must do the following:

- Boot a DOS operating system from diskette.
- Create and format a small DOS partition on the first physical drive (C:) and make it bootable.
- Load the basic NetWare kernel (SERVER.EXE).
- Run the NetWare installation utility (INSTALL.NLM)
- Access the ADSM server through a TCP/IP connection.
- Run the NetWare ADSM client.

The set of bootable diskettes for NetWare Version 3.12 server recovery consists of two 1.44 MB diskettes and a backup copy of the ADSM NetWare client installation diskette(s).

Create Disk 1

- **Create Disk 1 as DOS bootable**

  Use the DOS FORMAT command with the /S option to create a 1.44 MB bootable diskette (mark it disk 1). You may also want to specify the /V option to write a label on the diskette. Formatting can be done on any machine booted with a DOS system. This includes the current Novell NetWare server machine, though to format it you must bring down the server and return it to the DOS prompt. Of course, the FORMAT command must also exist on the C: drive.

  Disk 1 should now contain the following files:

  ```
  COMMAND.COM
  IBMBIO.COM      (hidden)
  IBMDOS.COM      (hidden)
  ```

  Note: You will not see the hidden files, using normal DOS commands like DIR. The extension of the DOS modules depends on the type of DOS used. We used the extensions in IBM PC DOS. Other DOS vendors may come with different types of extensions, for example, .EXE.

- **Add DOS files**

  Copy the following DOS files to disk 1:

```
CHKDSK.COM
DOSKEY.COM
EDIT.COM
FDISK.COM
FORMAT.COM
LABEL.COM
MORE.COM
SYS.COM
```

Note: Not all of the DOS modules listed above are essential, but we include them for flexibility and ease of use. For brand new drives, the FDISK and FORMAT commands are a must. The EDIT command will come in handy if you have to modify ASCII files (for example, .BAT or .NCF files) during the recovery.

- **Add NetWare files**

  Copy the following NetWare files to disk 1:

  ```
  SERVER.EXE
  STARTUP.NCF
  ```

  A typical STARTUP.NCF file contains these entries:

  ```
  LOAD PS2SCSI SLOT=1
  SET RESERVED BUFFER BELOW 16 MEG=200
  ```

- **Add Disk and LAN drivers**

  Copy the NetWare disk and LAN drivers used to disk 1. Refer to the information you have collected as described in 11.2, “Predisaster Preparation: Bootable Diskettes” on page 172 about the NetWare disk and LAN drivers used by the server. If more space is required, copy the remainder to disk 2.

  Some commonly used NetWare drivers for IBM PS/2s or PCs are:

  ```
  IDE.DSK     (for normal IDE drive)
  PS2SCSI.DSK (for IBM SCSI drive on IBM MCA PC)
  TOKEN.LAN   (for IBM Token ring)
  ```

- **About CONFIG.SYS and AUTOEXEC.BAT**

  You typically are not required to use CONFIG.SYS for a NetWare server machine unless DOS requires the loading of a vendor-provided disk driver to access the C: drive. In this case, copy the CONFIG.SYS and the required disk driver to disk 1. You may also want to modify the path statement in the CONFIG.SYS file to point to the root directory.

  To keep the recovery process simple, comment out statements in the AUTOEXEC.BAT and CONFIG.SYS files that will not be used in the recovery process. For example, if the AUTOEXEC.BAT includes statements to load the SERVER.EXE, comment them out.

Create Disk 2

- Format a 1.44 MB diskette and mark it as disk 2. You may want to use the /V option to put a label on this diskette. Do not include the /S option as it takes up unnecessary space on the diskette.
- **Create the TCPRECOV.NCF file**

  TCPRECOV.NCF enables you to set up the TCP/IP network, load the required TSA312.NLM, and start the ADSM client application all within a single command. Copy the current AUTOEXEC.NCF to disk 2 and rename it as TCPRECOV.NCF.

  Edit the TCPRECOV.NCF file by commenting out any statement that is not needed for the recovery process (see Figure 32).

  For installation that uses name space support, the LOAD namespace.NAM statements are normally coded in the AUTOEXEC.NCF. Leave these statements in the TCPRECOV.NCF file.

  Note: If name space other than DOS is used, and no LOAD namespace.NAM statements are coded in either the AUTOEXEC.NCF or STARTUP.NCF file, code them in this TCPRECOV.NCF file.

  To include some cleaning up capability in TCPRECOV.NCF, it may be a good idea to include some UNLOAD statements (before any LOAD statement) in the TCPRECOV.NCF file. An example is UNLOAD ACPWTCPS. This UNLOAD statement removes the ACPWTCPS stub in the storage. This can be helpful in cases when the loading or binding of TCPIP has failed (for whatever reason) and you have to rerun TCPRECOV.NCF. The presence of the ACPWTCPS stub in storage may prevent other modules (such as ADSM) from loading.

```
LOAD TOKEN FRAME=TOKEN-RING_SNAP NAME=TOKEN-IP
LOAD TCPIP
BIND IP TO TOKEN-IP ADDR=129.33.160.33
     MASK=255.255.255.0 GATE=129.33.160.254
MOUNT ALL
LOAD TSA312
SEARCH ADD SYS:/ADSM
LOAD DSMC
```

Figure 32. Sample TCPRECOV.NCF File: NetWare 3.12

- **Add NetWare files**

  Copy the following NetWare files to disk 2:

```
A3112.NLM
AFTER311.NLM
CLIB.NLM
EDIT.NLM
INSTALL.NLM
IPXS.NLM
MATHLIBC.NLM
MSM31X.NLM
ROUTE.NLM
SMDR.NLM
SMDR31X.NLM
SNMP.NLM
SPXS.NLM
STREAMS.NLM
TCPIP.NLM
TLI.NLM
TOKENTSM.NLM
TSA312.NLM
```

Copy any name space module used, such as MAC.NAM.

If you run out of space, you may have to copy the remainder onto a third formatted diskette (disk 3).

Note: After successfully testing the diskettes created, you can use any available zipping tool to save diskette space or even to create self-install and extract diskettes. The additional steps involved are not discussed here.

Create Copy of ADSM Client Diskettes:

Use the DOS DISKCOPY command or any other DOS utility to make a duplicate copy of the ADSM NetWare client installation diskettes.

11.3 Postdisaster Recovery Using Bootable Diskettes

In this section we describe how to recover a Novell NetWare Version 3.12 server from a disaster using the information we saved prior to disaster (described in 11.2, “Predisaster Preparation: Bootable Diskettes” on page 172) and the bootable diskettes we created (described in 11.2.3, “Creating the Bootable Diskettes” on page 174).

To simulate a disaster to the original Novell NetWare server, we “trashed” it and then used a completely different set of replacement hardware for the recovery.

In preparation for the disaster, we recommend that you do the following:

1. Collect and save information about the ADSM client platform to aid in any future postdisaster re-creation of the hardware environment.

2. Take a complete ADSM backup of the client files.
3. Create bootable diskettes for the specific NetWare server.

After you have completed the preparatory steps, after a disaster to the ADSM client, you are positioned to begin the bare metal restore.

11.3.1 Rebuild the Hardware Environment

Retrieve information about the Novell NetWare server machine to help re-create the hardware environment of the destroyed ADSM client; the new replacement machine must have a similar configuration (for example, volumes are not mirrored or duplexed).

If you used DRM as the repository for information about the Novell NetWare server machine, retrieve it by issuing the appropriate ADSM queries to the ADSM server. For examples of these queries, see 1.3.6, “Disaster Recovery Manager” on page 18.

11.3.2 Boot the Recovery System

Use the NetWare Version 3.12 bootable diskettes to boot the replacement hardware and prepare for ADSM file recovery. Follow steps listed below.

Note: We made the assumption that all NetWare-related files on the C: drive are stored in a directory other than the root directory. We used C:\SERVER.312 as our directory.

11.3.2.1 Step 1: Boot the New Machine from Disk 1

Boot the new machine from disk 1.

11.3.2.2 Step 2: Create a Small DOS Partition

If there is already a small DOS partition on the first drive and its size is adequate, you can skip this step. Do not use an unnecessarily large size for the DOS partition. Set aside enough free space for the NetWare partition.

Run the DOS FDISK command to create a DOS partition on the (first) drive. Use the size you recorded before the disaster. Once you have changed the partition, you have to reboot the machine when you exit FDISK. Leave disk 1 in the diskette drive.

11.3.2.3 Step 3: Create a Bootable DOS Partition (C: Drive)

If the DOS partition is already bootable or formatted, you may not want to reformat it. However, DOS modules are version sensitive, so we recommend that you transfer the DOS system files from disk 1 to the C: drive. To transfer the files, issue this command:

```
SYS C:
```

Transferring ensures that both the DOS system on the C: drive and those DOS files to be copied over later are at the same level.

If the DOS partition has just been created, format it with the /S and /V options:

```
FORMAT C: /S/V
```

/V is optional. If used, you are prompted to specify a label for the drive at the end of the formatting. You may, however, choose not to provide a label. You can also use the LABEL command to change the label of a drive at any time. The command syntax is:

```
LABEL C:
```

11.3.2.4 Step 4: Copy Files on Disk 1 to the C: Drive

If you want to put all NetWare files on the C: drive's root directory, issue the COPY command:

```
COPY A:*.* C:\
```

and go to Step 5.

Otherwise, put all NetWare files on the C:\SERVER.312 directory. To create this directory and make it the current directory, issue these commands:

```
MD C:\SERVER.312

CD C:\SERVER.312
```

Copy all NetWare files from disk 1 to this directory, that is, move all files with extensions of LAN, DSK, NCF, or NLM. Copy SERVER.EXE to disk 1. For example:

```
COPY A:TOKEN.LAN  C:
```

Copy the DOS files (including CONFIG.SYS and AUTOEXEC.BAT) to the root directory. You can use a wild card for the group copying:

```
COPY A:*.COM C:\
```

11.3.2.5 Step 5: Copy Files on Disk 2 to the C: Drive

To copy the contents of disk 2 to the C: drive, issue this command:

```
COPY A:*.* C:
```

If you used additional diskettes to hold the .NLM files, remember to copy them over to the C: drive.

11.3.2.6 Step 6: Modify the CONFIG.SYS and AUTOEXEC.BAT Files

If CONFIG.SYS exists and is copied, make sure the path statements in it are changed to point to the C: drive instead of A: (the diskette drive). Use the EDIT command to modify the file:

```
EDIT C:\CONFIG.SYS
```

Do the same for the AUTOEXEC.BAT file. This is also a good time to comment out the unnecessary statements in these files. Make sure the AUTOEXEC.BAT does not load the SERVER.EXE.

11.3.2.7 Step 7: Reboot the System from the C: Drive

Remove any diskette in the diskette drive and reboot the system. The machine should come up as when you booted it with disk 1, except with the C:> prompt displayed instead.

11.3.2.8 Step 8: Load NetWare Kernel SERVER.EXE

If you have put all NetWare files in a particular directory, set it as the current directory:

```
CD \SERVER.312
```

Start the server without loading the AUTOEXEC.NCF file; use this command:

```
SERVER -NA
```

You are asked to specify the Server's Name and the Server's IPX internal network number. Respond with the information you recorded for this server before the disaster.

11.3.2.9 Step 9: Create the NetWare Partitions

Load the NetWare installation utility (INSTALL.NLM) from the server console:

```
LOAD INSTALL
```

From the **Installation Options** menu, select **Disk Options**.

From the **Available Disk Options** menu, select **Partition Tables**.

The next menu displayed shows the available disk drives accessible to NetWare.

Note: If you do not see as many disk drives as you expect, the most likely explanation is that all of the required NetWare disk drivers have not been loaded.

Move the cursor to highlight the disk drive where you want to create the NetWare partition and press <ENTER>.

Note: The first NetWare partition does not have to be on the first physical drive.

Two panels are displayed. One, as background, shows partition information for the drive selected, for example, Types/Sizes of partitions that have already been defined and free space information. (If a NetWare partition has been defined, or no more free space is available on this drive, you will not be able to define one.)

On the other panel (Partition Options) you can create or delete a NetWare partition. Select **Create NetWare Partition**.

On the Partition Information panel you can specify the partition size by cylinder (not by capacity). Refer to the information you have recorded for this server before the disaster. It may be a process of some trial and error to get the correct size.

Leave the Hot Fix set at 2.0%. In this case, the actual partition size available for NetWare volumes is only 98% of the size defined.

Press <ESC> and reply YES to create the partition.

Do the same to create other partitions for this server.

11.3.2.10 Step 10: Create the NetWare Volumes

From the Installation Options menu, select **Volume Options**.

The Volumes menu displayed will have no blank entry because a NetWare volume has not been defined at this stage.

Press <INSERT> to create a new volume. NetWare always defaults the first volume defined to SYS. It also always assumes that you want to use all of the free space when you define a volume. Refer to the information you recorded for this server before the disaster and specify the Volume Block Size and the Volume Size.

Note: You cannot specify the volume size directly. Change the Initial Segment Size field to get the correct size.

Press <ESC> and reply YES to create this volume. You are asked to "wait" while NetWare formats the volume.

Do the same to create all other volumes for the server. You must create the volume before starting the ADSM restoration for a volume.

11.3.2.11 Step 11: Mount the SYS Volume

The Volume Options panel shows all of the volumes defined. Highlight the SYS volume and press <ENTER>. The Volume Information panel will appear as before, but you will be able to move the cursor to the Status field this time. The status should show ***Not Mounted***.

Move the cursor to the status field and press <ENTER>. Select **Mount Volume** from the Volume Status panel and press <ENTER>.

After NetWare successfully mounts the volume, it updates the status of the volume to ***Mounted***.

You do not have to mount the other volumes at this time. They will be mounted when you issue the TCPRECOV.NCF command (see Step 15).

11.3.2.12 Step 12: Add DOS Path to the Server's Search Path

Once NetWare has mounted the SYS volume, it will change its search path to SYS:\SYSTEM. You can display the NetWare search path any time by issuing the SEARCH command from the server console. If you are currently not at the console screen, switch to that screen either by toggling around (use <ALT>+<ESC>) or selecting directly after pressing <CTRL>+<ESC>.

Add the DOS directory where the NetWare files are kept to the search path:

```
SEARCH  ADD  C:\SERVER.312
```

or

```
SEARCH  ADD  C:\
```

11.3.2.13 Step 13: Install the ADSM NetWare Client

Insert the ADSM NetWare Client installation diskette into the A: drive (these should be disk 3 and disk 4, which we made by taking a DISKCOPY of the ADSM NetWare Client installation diskettes).

From the server console, enter:

```
LOAD  A:\INSTDSM
```

There are three installation options. You do not have to install the API code at this time. Installation of SMS modules is optional as the NLMs were also copied to disk 2. The sequence of installing ADSM and SMS modules is immaterial.

You are prompted to specify the target directory for both cases. For the ADSM client code, you can define the target directory of your choice. For the SMS modules, we recommend that you use the default directory,

SYS:\SYSTEM

. We used the default directory for both cases.

After installation, add the new paths to the NetWare's search path:

```
SEARCH  ADD   your_directory
```

We chose to add the search path (SYS:\ADSM) in the TCPRECOV.NCF file.

11.3.2.14 Step 14: Create the ADSM NetWare Client Options File

Load the EDIT NLM from the server console:

```
LOAD  EDIT
```

In the File To Edit window, enter:

```
SYS:\ADSM\DSM.OPT
```

(or use the path of your choice).

Reply YES to create.

On the blank screen, type in the following values for your server setup:

```
NODENAME           ADSM_nodename_for_this_client
COMMMETHOD         TCPIP
TCPSERVERADDRESS   the_ADSM_server_IP_address
TCPPORT            the_ADSM_server_TCPIP_port
```

For example, the DSM.OPT we used looked like this:

```
NODENAME           ITSC312A
COMMMETHOD         TCPIP
TCPSERVERADDRESS   129.33.160.100
TCPPROT            1500
```

Press <ESC> and reply YES to save this file.

11.3.2.15 Step 15: Bring Up TCP/IP and Start the ADSM Application

All of the required commands are precoded in TCPRECOV.NCF, which is on the DOS C: partition. If you have to review or modify its contents, use the NetWare EDIT command.

Issue the TCPRECOV command from the server console:

```
TCPRECOV
```

When the ADSM application is successfully loaded, the **DSMC>** prompt is displayed, and you are ready to issue ADSM client commands.

Note: If name space other than DOS is used, you can add the required name space support (using server console command ADD NAME SPACE) at this time. For example:

```
ADD NAME SPACE MAC TO SYS
```

At this point, you can also check and verify the status of the TCP/IP network by issuing the NetWare **CONFIG** command from the server console.

11.3.2.16 Step 16: Rebuild the NetWare Server

You are now ready to start file restoration, using ADSM. To check the active backups stored at the ADSM server for this client, enter the following at the ADSM> prompt:

```
QUERY VOLUME
```

You are prompted to provide the password for the node name specified in the DSM.OPT file. You must provide the correct password to be able to proceed further. If the correct password is not part of the information recorded before the disaster, the ADSM administrator can change the ADSM password.

The active volume backups, including the bindery, will be displayed (provided you have followed the predisaster preparation recommendations outlined in 11.2, “Predisaster Preparation: Bootable Diskettes” on page 172 and they exist!).

The first file to restore is the bindery. Issue this ADSM command:

```
RESTORE -REPLACE=YES BINDERY
```

For the first time round, you are asked to enter the NetWare user for this node. Reply ***supervisor***. Press <ENTER> when NetWare requests the password for this user.

If you do not specify the ***REPLACE*** option, you are prompted to either replace or not replace the current bindery. Reply YES. After the bindery is successfully restored, rebuild the SYS volume:

```
RESTORE -REPLACE=NO -SUBDIR=YES -VOLINFORMATION SYS:*
```

Restore the original DSM.OPT from the ADSM backup:

```
RESTORE -REPLACE=YES SYS:ADSM\DSM.OPT
```

Restore the original AUTOEXEC.NCF from the ADSM backup:

```
RESTORE -REPLACE=YES SYS:SYSTEM\AUTOEXEC.NCF
```

Restore any other NetWare volume, using the same command. Replace the SYS with the respective volume name, for example, APPL, VOL1.

11.3.2.17 Step 17: Restart the Server

You are now ready to restart the recovered Novell NetWare 3.12 server. Before you shut down the server, first verify that the restored AUTOEXEC.NCF file correctly describes your current machine setup (for example, check the disk and LAN drivers and the slot-number used).

There are at least two ways to edit the AUTOEXEC.NCF file on the SYS:\SYSTEM directory. Either use the NetWare EDIT module as described earlier or go through the Installation Options panel to pick the System Options and select the **Edit AUTOEXEC.NCF File** option.

From the server console, enter: **DOWN**. After the server is shut down, type **EXIT** to return the machine to DOS.

At this point you may want to restore the original CONFIG.SYS: and AUTOEXEC.BAT files by uncommenting all lines you commented out when you prepared the bootable diskettes. You may also want to reinsert the SERVER.EXE statement in the AUTOEXEC.BAT file so that the NetWare server will be started automatically.

Restart the server, using your normal procedure.

Login as administrator to verify the file system and trustee assignments.

You may also want to run the BINDFIX utility to ensure that the restored bindery is at a consistent state. Refer to NetWare 3.12 documentation if you need more information regarding BINDFIX utility.

If you had files and programs stored on the base boot-up C: DOS partition which was outside the scope of the backups we discussed here, but for which you may have kept a separate backup, you can restore them now. You have to shut down the server and return to DOS.

At this point, you may also want to reinstall the updates or PTFs for the ADSM NetWare Client.

Optional - Using NWSHELL

We did not use NWSHELL.NLM, a Software Developer's Kit from Novell, but include the instructions here for your reference.

If you have access to NWSHELL.NLM you do not need the ADSM NetWare Client Installation diskettes. To use NWSHELL, you have to create a new diskette with the following ADSM files:

```
ACPSAAS1.NLM
ACPSAAS2.NLM
ACPWSRVS.NLM
ACPWTCPS.NLM
DSCAMENG.TXT
DSMC.NLM
DSMC.HLP
DSMC.NCF
DSM.OPT
```

All these files reside in SYS:\ADSM. You must also copy the NWSHELL.NLM, either onto this diskette or one of the other two.

Using NWSHELL saves you the steps of installing the ADSM client code and creating the DSM.OPT file.

During the NetWare recovery, instead of reinstalling the ADSM client, load NWSHELL from the server console. NWSHELL creates a DOS-like session with the supervisor as the user. In normal operation, you are prompted for the supervisor's password. For the recovery case, because the bindery is yet to be built, there will be no prompt.

NWSHELL assigns drive 0: as SYS: and 9: as SYS:\SYSTEM. It also makes 0: the current drive.

You can issue DOS-like commands from the screen, for example, DIR or COPY. A HELP command is also available.

Create the SYS:\ADSM directory and make it the current directory; that is, from 0:> , enter MD ADSM, then CD ADSM.

Copy all files on the new diskette to this directory.

Note that copying under this shell is a very slow process and is not always successful.

11.4 Recovery with Bootable Diskettes and ADSM Peer: Predisaster Preparation

In the previous section we outlined the steps to recover a Novell NetWare Version 4.10 server to the point where it could begin the ADSM client restore using TCP/IP communications to the ADSM server.

In this section we talk about an alternative method to perform ADSM restore when there is no direct TCP/IP link between the destroyed NetWare ADSM client and its ADSM server. This may be the case where SNA LU 6.2 was used or there is no direct communication link between the ADSM client and the server.

NetWare servers are normally linked together and capable of exchanging data among themselves through the NetWare's SMS interface using the IPX/SPX communication protocol. ADSM takes advantage of the feature and supports this capability of NetWare's SMS. A NetWare ADSM client can therefore perform ADSM backup/restore services on behalf of its logically linked peer, which may or may not have a direct connection to the ADSM server (see Figure 33 on page 189). In other words, as long as the link between the gateway NetWare Client and the ADSM server is not broken, it is always possible to recover a crashed NetWare server regardless of whether a direct communication link is available.

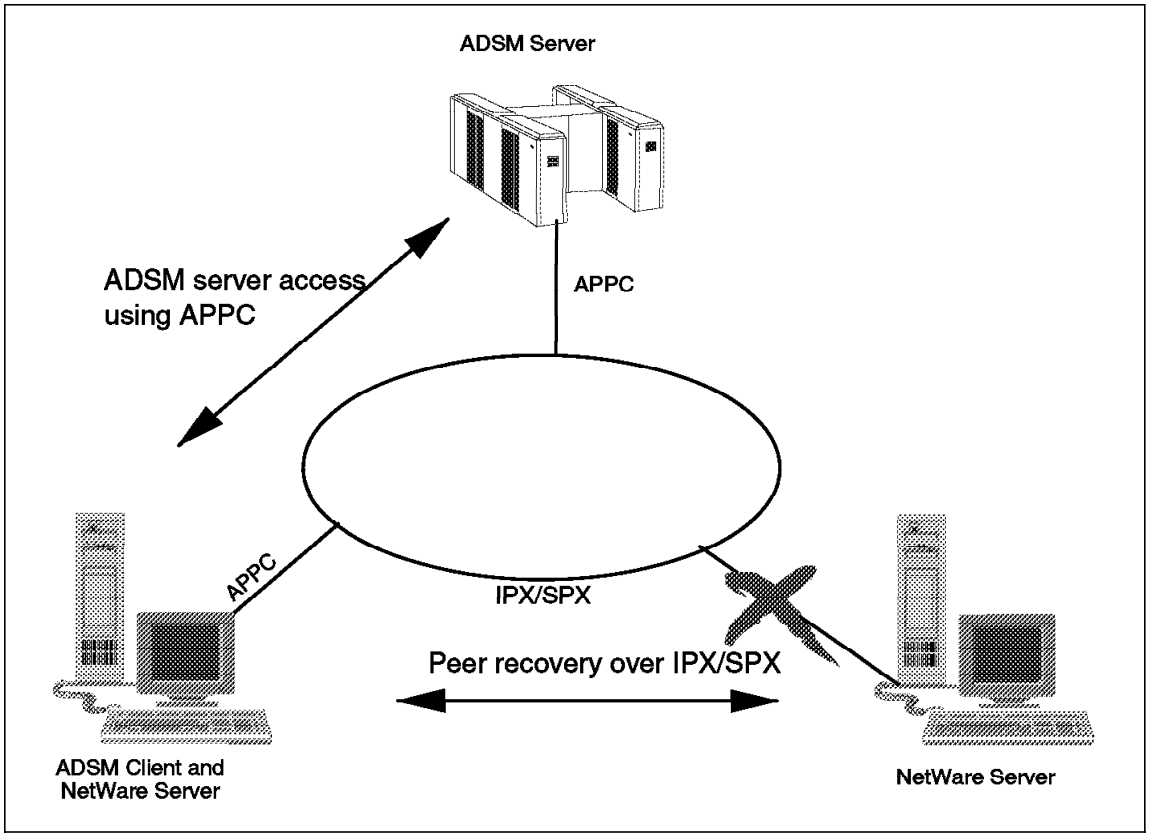


Figure 33. Using a Peer NetWare 3.12 Server to Perform Proxy ADSM Recovery

Note: Of course, a direct connection between the ADSM client and server is always preferable from a network and server performance standpoint. So you would only use this method if you had no alternative in a disaster recovery situation.

11.5 Predisaster Preparation: Peer Recovery

The information we recommend you save before the disaster for this method is the same as that described in 11.2, "Predisaster Preparation: Bootable Diskettes" on page 172 with the following exceptions:

- **Add**

  Because you will be using IPX instead of TCP/IP to facilitate the ADSM restore, you have to save the *IPX external network number* used when joining the physical network. (Note: This is different from the *IPX internal network number*.) You can obtain this information from the AUTOEXEC.NCF file or by using the CONFIG server command and

looking under ***LAN protocol : IPX network...*** Add this information to the other data you are saving in preparation for disaster.

After you use the bootable diskettes and the proxy ADSM recovery by a peer Novell NetWare server, the assumption is that you will want to reestablish communications between the restored ADSM client and the ADSM server. So record any specific information (for example, for an SNA LU 6.2 implementation) your installation will require.

- **Delete**

  Because you will be using IPX instead of TCP/IP and depending on a peer Novell NetWare server for its ADSM client, information related to the use of TCP/IP and ADSM is not required (though it certainly does not hurt to record it anyway).

11.5.1.1 Authorize a Peer Novell NetWare Server ADSM Client to Restore

Before the disaster, you must authorize the peer Novell NetWare ADSM client to restore your ADSM backups. For example, if one Novell NetWare ADSM client, PEIXIANG, wants another Novell NetWare ADSM client, PEICHONG, to have the authorization to restore his backups, he would use the following ADSM command:

```
SET ACCESS BACKUP * PEICHONG
```

If ADSM client PEIXIANG wants to check who has been authorized to restore his backups, he would use the following ADSM command:

```
QUERY ACCESS
```

11.5.1.2 Create the NetWare Bootable Diskettes

Create the NetWare bootable diskettes, using the procedure outlined in 11.2.3, “Creating the Bootable Diskettes” on page 174, with the following differences:

Optional: If you want, you can make the following modifications (though if you do not, these elements will not be used):

- ADSM client installation diskettes not required

  Because you are depending on a peer Novell NetWare ADSM client to perform the ADSM restore on our behalf, you can choose not to include the copies of the ADSM NetWare client installation diskettes.

- These NLMs no longer required

  For the same reason, the following NLMs need not be copied to disk 2 of the bootable diskettes:

```
TCPIP
SNMP
IPXS
MATHLIBC
```

Mandatory: The TCPRECOV.NCF file (see Figure 32 on page 177) is valid for using a TCP/IP connection only. Modify this file to reflect the IPX communications you intend to use to communicate with the peer Novell NetWare server. To eliminate confusion, rename this file to IPXRECOV.NCF. Figure 34 shows the contents of a sample file.

```
LOAD TOKEN NAME=TOKEN-IPX
BIND IPX TO TOKEN-IPX NET=00000002
MOUNT ALL
LOAD TSA312
```

Figure 34. Sample IPXRECOV.NCF File: Netware 3.12

11.6 Postdisaster Recovery Using Peer Recovery

The steps to do bootable diskette recovery with an ADSM Peer Novell NetWare server are very much like those described in 11.3, “Postdisaster Recovery Using Bootable Diskettes” on page 178. Follow these steps until the SYS volume is mounted and the DOS path is added to the server′s search path.

Next, bring up the IPX/SPX network. We prepared the necessary commands in our IPXRECOV.NCF file (see Figure 34.). If you have to edit this file, use the NetWare EDIT command. To start the network, issue the IPXRECOV command from the server console.

To check the network status, use the CONFIG server command.

Now that you have established IPX communications with the peer Novell NetWare server, you are ready to use its ADSM client to rebuild the files on the newly booted Novell NetWare server:

- Start the ADSM client on the peer Novell NetWare server.
- From the ADSM prompt, issue the ADSM command to restore the bindery on behalf of the newly booted, but currently ADSM clientless, Novell NetWare server called PEIXIANG. If you call its peer Novell NetWare ADSM client PEICHONG, that will be doing the ADSM restore, the ADSM command that PEICHONG would issue is:

```
RESTORE -FROMNODE=PEIXIANG PEIXIANG\BINDERY: -REPLACE=YES
```

After entering this command, you are prompted for the ADSM password to start a session with the ADSM server. You are also asked to enter the NetWare userid of the target server - use **supervisor**, and for the password just press <ENTER>.

After the bindery is restored, rebuild the SYS volume:

```
RESTORE -FROMNODE=PEIXIANG PEIXIANG\SYS: -REPLACE=YES
-SUBDIR=YES -VOLINFORMATION
```

Continue to restore the other volumes in the same way. Once you are finished, you can restart the Novell NetWare server. If you have to modify the AUTOEXEC.NCF file, use the NetWare EDIT command or access the file through the Installation Options panel.

Shut down the recovered server and exit to DOS (enter **DOWN** and then **EXIT** from the console)

At this point you may want to restore the original CONFIG.SYS and AUTOEXEC.BAT files. You may also want to reinsert the SERVER.EXE statement in the AUTOEXEC.BAT file so that the NetWare server will be started automatically.

Restart the server, using your normal procedure, and login as administrator to verify your server and file system.

You may also want to run the BINDFIX utility to ensure that the restored bindery is at a consistent state. Refer to NetWare 3.12 documentation if you need more information regarding BINDFIX utility.

If you had files and programs stored on the C: DOS partition, which was outside the scope of the backups we discuss here, but for which you may have kept a separate backup, you may restore them now. You have to shut down the server and return to DOS to do so.

At this point, you may also want to reinstall the updates or PTFs for the ADSM NetWare Client.

Chapter 12. Novell NetWare Version 4.10 Recovery

In this chapter we discuss some techniques to recover a Novell NetWare Version 4.10 server environment using bootable diskette recovery based on the approach described by Jerry Lawson of ITT Hartford.

Note:

The method developed here is for a NetWare Version 4.10 server in a single server environment only. Considerations for servers in a multi-server environment are not included here.

For a good reference to these considerations, refer to the document *ADSM Novell Directory Services (NDS) Backup and Recovery Guide* by Jim Smith that is shipped with the second diskette of the recent versions of code - L0.5 or V2 R1 L0.6f.

We examine the minimum resources and information required to build a base Novell NetWare Version 4.10 system that is capable of running an ADSM client using a TCP/IP connection to the ADSM server. We document the steps to create the bootable diskettes and walk through the recovery of a Novell NetWare Version 4.10 server using these bootable diskettes to initiate the ADSM recovery.

We also discuss a bare metal restore of Novell NetWare Version 4.10 servers that uses the bootable diskettes, but in conjunction with a peer Novell NetWare server which is used to do the ADSM recovery. This is an alternative method for those Novell NetWare ADSM clients that do not use TCP/IP to communicate with their ADSM servers (perhaps they have NetWare for SAA installed and use SNA APPC instead or there is no direct link with the ADSM server at all).

Note: The techniques described here do not include recovery of any files or programs you store on the DOS partition. If you do have the need to recover this DOS partition, you can refer to the technique described in Chapter 7, “DOS/Windows Version 3.1 Recovery” on page 125.

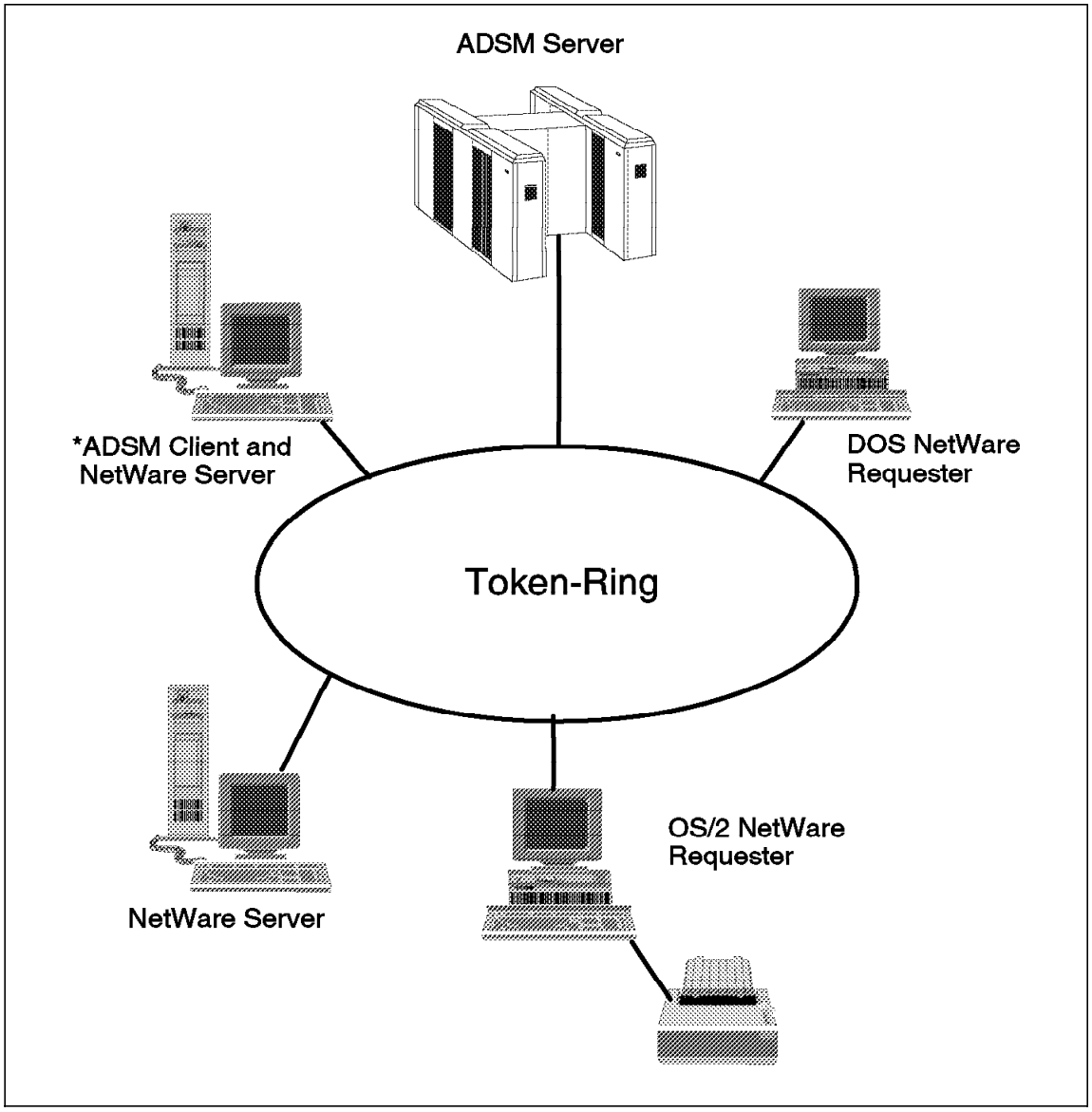


Figure 35. Recovering the NetWare Version 4.10 Server and ADSM Client

12.1 Product Overview

This section gives a brief overview of the Novell NetWare Version 4.10 system. For a detailed description of this operating system, refer to the Novell NetWare 4.10 publications.

12.1.1 NetWare Version 4.10 Operating System

Novell NetWare Version 4.10 is a 32-bit network operating system (NOS). It is regarded as a client-server operating system providing services to workstations (clients). These services include login and authentication services, file services, messaging services, print services, and routing services.

Besides retaining most of the core and architectural features of the NetWare 3.12 system, NetWare 4.10 includes many new enhancements. (For a brief overview of NetWare 3.12 system see 11.1, “Product Overview” on page 168.) Of the many advanced features implemented, the most significant change is the Novell NetWare directory services (NDS), first introduced in the NetWare 4.0 system. (NetWare 4.0 and 4.02 preceded the NetWare 4.10 system.) NDS replaces the bindery used in the pre-Version 4 NetWare systems.

As with NetWare 3.12, NetWare 4.10 needs DOS to start up its base kernel, SERVER.EXE.

12.1.2 Novell Directory Services

NDS keeps track of network users, servers, and all other available resources of the network in a database known as the Directory Information Base. Implementation of this *global* database conforms to the International Organization for Standards (ISO) X.500 specification. Unlike a typical information database, NDS refers to records as *objects* and fields of records as *properties*. For example, a user (record) is called an *object*, whereas the login name, full name, and contact number (fields) are called the *properties* of the object.

Objects (network users, resources) are organized into a hierarchical tree structure known as the directory tree. On top of this tree is the root object, which forms the base of the directory. The root object usually carries the same name as the organization′s name.

Besides the root object, there are *leaf* objects, which represent the users and resources, and *container* objects. Container objects are like branches of a tree. They hold the leaf objects and other container objects.

Associated with objects in the directory tree, as well as directories and files in the file system, are the access *rights*. There are four types of rights in a NetWare 4.10 system: *object, property, directory*, and *file*. These rights determine how one object (for example, a user) can access other objects (resources) in a system. Rights are assigned to objects by an administrator. When an object is given rights to another object, it becomes the *trustee* of that object. The trustee assignments of an object, known as the **trustee list**,

keeps track of who the trustees are. This list is stored as part of the object's access control list (ACL) property in the NDS.

NDS is a distributed database. It can be partitioned and stored in a number of servers across the network. Each partition then becomes a subtree of the entire NDS directory tree. The partitioning of NDS allows related information in the NDS to be put together into a subtree that can be placed on a server that is closer to the users who are accessing it. This helps cut down the network traffic.

For fault tolerance reasons, partitions are typically replicated. It is common for each partition to have more than two replicas. This setup not only prevents the loss of a partition due to a disk failure but also helps to improve the network access as replicas can be placed on servers closer to users who need it.

Distributed partitions and replicas are updated constantly. This ongoing synchronization process ensures that the integrity of the NDS is maintained.

For an in-depth discussion of NDS and how it works, refer to such Novell publications as *NetWare 4 Introduction to NetWare Directory Services* and *NetWare 4 Supervising the NetWare*.

12.2 Bare Metal Recovery With Bootable Diskettes: Predisaster Preparation

The disaster we are preparing for is the total and catastrophic loss of the ADSM client, where provision has to be made to restore everything from the bare metal up. If our disaster recovery preparations can cover this worst case scenario, we can assume that they will also be able to handle recovery from lesser disasters.

In this section we discuss the information to collect and save before a disaster to enable a bare metal restore.

12.2.1.1 ADSM Backups

We recommend that the directory and all volumes (including the volume restrictions and trustee directory assignments) are included in the ADSM backup that will eventually be used for the ADSM restore part of the bare metal recovery of the Novell NetWare server platform.

For more information about ADSM backups, have a look at *Getting Started with ADSM NetWare Clients*, GG24-4242.

12.2.1.2 Operating Environment of the ADSM Client

In preparation for disaster recovery we recommend that you collect and save offsite the information listed below in addition to the ADSM backup data. Depending on your installation, you could save this information by using the DRM feature, or you could save it on hardcopy stored offsite. The way in which you save the information is not as important as ensuring that it is saved **somewhere** where it can be easily retrieved along with the client recovery media when a disaster occurs.

- **Software Configuration**

  Save information about the version of DOS you are using. To check the DOS version currently installed on the NetWare server, bring down the server (use the DOWN command from the server console) and exit to DOS (use the EXIT command). It is not necessary to use the same level or vendor of DOS as on the working server to build the bootable diskettes. If a different DOS version is used, however, that version will be the DOS version for the newly recovered server.

  Record whether boot manager is installed on the C: drive. DOS does not support the management of the boot manager partition. If the boot manager partition is mandatory for the machine, you will need (bootable) diskettes from other operating systems (for example, OS/2) or vendor products that provide this utility, as well as the documentation explaining its use.

- **Hardware Configuration**

  Record the size of the C: drive. You have to bring down the server to be able to check the capacity of the C: drive with FDISK or CHKDSK. Depending on how the NetWare system was originally installed, you may need a slightly bigger C: drive to house all files from the bootable diskettes. A size of 5 MB is ideal.

  If a specific disk driver is required for DOS to access the drive, note it. You can check this from the CONFIG.SYS file. Be aware that you may not be using the same type of disk in your recovery hardware.

  Use the NetWare install utility, INSTALL.NLM, to collect the following information:

  - Number of partitions in the server and their respective sizes
  - Capacity of the SYS volume
  - Block size used for the SYS volume
  - Similar information for any other volumes on the server

  Record all disk and LAN drivers used. You can get this information from the STARTUP.NCF and AUTOEXEC.NCF files. During the actual

recovery, you may not always be able to use the exact same make of hardware. If different types of disk or LAN drivers are used for the new replacement machine, the required drivers for both DOS and NetWare must be available.

If a name space other than DOS is used, record this information also. Use the VOLUMES console command to list the name space added to each of the volumes.

- **Directory tree and bindery context details**

  Besides recording the NetWare server's name and the IPX internal network number, note the directory tree name and the bindery contexts set up for this server. Use the CONFIG server command to get this information.

  If the server has a vendor product installed to extend the schema, note this. The schema is currently not backed up by SMS/ADSM. You have to reinstall the product to re-create the schema extension after the server is recovered.

- **Communications details**

  Record the TCP/IP address and the gateway TCP/IP address used by this server. This information is recorded in AUTOEXEC.NCF. You can also get the same information from the server console by issuing the CONFIG command. To get this network information from the server console, the corresponding network has to be started first.

  The TCP/IP information for the ADSM client will be required only at later stages of the server recovery when files from the bootable diskettes can be accessed and copied. So this information can be precoded in an NCF (we used TCPRECOV.NCF) and run from the server console.

  Record the ADSM server's TCP/IP address and TCP port address, as well as the ADSM client node name. This information can be found in the client options file (DSM.OPT) in the SYS:/ADSM directory.

  Note: Depending on your installation, you can also record the password associated with the ADSM client node name. You may prefer, for reasons of security, to simply reset all ADSM client passwords if you cannot remember them.

In summary, this is the information you should collect:

- DOS version
- Size of the C: drive
- DOS disk driver (if any)
- Is boot manager installed on this C: drive? (Y/N)

- Number of partitions in this server and their respective size
- Capacity of the SYS volume
- Block size used for the SYS volume
- Similar information for other volumes on the server
- Disk and LAN drives used
- Name spaces used
- Server name
- Server IPX internal network number
- Server TCP/IP address
- Directory tree name
- Bindery contexts
- OEM product installed to extend the schema
- Gateway TCP/IP address used by the server
- ADSM server′s TCP/IP address
- ADSM server′s TCP port address
- NetWare′s ADSM client node name and password

12.2.2 Creating the Bootable Diskettes

In this section we describe a method to create bootable diskettes for Novell NetWare Version 4.10. The method described here is based on the method provided by Jerry Lawson of ITT Hartford.

We tested this technique, using the following configuration:

- PC 360 with 32 MB of RAM
- 16 Mbps token-ring attachment
- 1 GB hard disk, partitioned with a 50 MB DOS partition, with the rest of free space for the NetWare partition
- Novell NetWare Version 4.10
- ADSM NetWare Version 2, Release 1 client code
- ADSM/AIX Version 2, Release 1, Level 0.2 server code

To rebuild a Novell NetWare Version 4.10 system from bare metal that is capable of restoring backup data from the ADSM server through a TCP/IP connection, you must be able to do the following:

- Boot a DOS operating system from diskette.

- Create and format a small DOS partition on the first physical drive (C:) and make it bootable.
- Load the basic NetWare kernel (SERVER.EXE).
- Run the NetWare installation utility (INSTALL.NLM)
- Access the ADSM server through TCP/IP connection.
- Run the NetWare ADSM client.

The set of bootable diskettes for NetWare Version 4.10 server recovery consists of three 1.44 MB diskettes, a backup copy of the ADSM NetWare client installation diskettes, and the original Novell NetWare 4.10 license diskette for the server.

12.2.2.1 Step-by-Step Instructions

Create Disk 1

- **Create Disk 1 as DOS bootable**

  Use the DOS FORMAT command with the /S option to create a 1.44 MB bootable diskette (mark it disk 1). You may also want to specify the /V option to write a label on the diskette. Formatting can be done on any machine booted with a DOS system. This includes the current Novell NetWare server machine, though to format it you must bring down the server and return it to the DOS prompt. Of course, the FORMAT command must also exist on the C: drive.

  Disk 1 should now contain the following files:

  ```
  COMMAND.COM
  IBMBIO.COM      (hidden)
  IBMDOS.COM      (hidden)
  ```

  Note: You will not see the hidden files, using normal DOS commands like DIR. The extension of the DOS modules depends on the type of DOS used. We used the extensions in IBM PC DOS. Other DOS vendors may come with different types of extensions, for example, .EXE.

- **Add DOS files**

  Copy the following DOS files to disk 1:

  ```
  CHKDSK.COM
  DOSKEY.COM
  EDIT.COM
  FDISK.COM
  FORMAT.COM
  LABEL.COM
  MORE.COM
  SYS.COM
  ```

Note: Not all of the DOS modules listed above are essential, but we include them for flexibility and ease of use. For brand new drives, the FDISK and FORMAT commands are a must. The EDIT command will come in handy if you have to modify ASCII files (for example, .BAT or .NCF files) during the recovery.

- **Add NetWare files**

  Copy the following NetWare files to disk 1:

  ```
  SERVER.EXE
  STARTUP.NCF
  ```

  A typical STARTUP.NCF file contains these entries:

  ```
  LOAD PS2SCSI SLOT=1
  SET RESERVED BUFFER BELOW 16 MEG=200
  ```

- **Add Disk and LAN drivers**

  Copy the NetWare disk and LAN drivers used to disk 1. Refer to the information you have collected as described in 12.2, “Bare Metal Recovery With Bootable Diskettes: Predisaster Preparation” on page 196 If more space is required, copy the remainder to disk 2.

  Some commonly used NetWare drivers for IBM PS/2s or PCs are:

  ```
  IDE.DSK     (for normal IDE drive)
  PS2SCSI.DSK (for IBM SCSI drive on IBM MCA PC)
  TOKEN.LAN   (for IBM Token ring)
  ```

- **About CONFIG.SYS and AUTOEXEC.BAT**

  You typically are not required to use CONFIG.SYS for a NetWare server machine unless DOS requires the loading of a vendor-provided disk driver to access the C: drive. In this case, copy the CONFIG.SYS and the required disk driver to DISK 1. You may also want to modify the path statement in the CONFIG.SYS to point to the root directory.

  To keep the recovery process simple, comment out statements in the AUTOEXEC.BAT and CONFIG.SYS files that will not be used in the recovery process. For example, if the AUTOEXEC.BAT includes statements to load the SERVER.EXE, comment them out.

Create Disk 2

- **Format a 1.44 MB diskette and mark it as disk 2**

  You may want to use the /V option to put a label on this diskette. Do not include the /S option as it takes up unnecessary space on the diskette.

- **Create the TCPRECOV.NCF file**

The TCPRECOV.NCF file enables you to load the required NLMs, set up the TCP/IP network, and execute the TSA NLMs, all within a single command.

Copy the current AUTOEXEC.NCF onto disk 2 and rename it as TCPRECOV.NCF.

Edit the TCPRECOV.NCF file and comment out any statement that is not needed for the recovery process (see Figure 36).

For an installation that uses name space support, the LOAD namespace.NAM statements are normally coded in the AUTOEXEC.NCF. Leave these statements in the TCPRECOV.NCF file.

Note: If a name space other than DOS is used and no LOAD namespace.NAM statement is coded either in AUTOEXEC.NCF or STARTUP.NCF file, code them in this TCPRECOV.NCF file.

```
LOAD CLIB
LOAD DSAPI
LOAD TOKEN FRAME=TOKEN-RING_SNAP NAME=TOKEN-IP
LOAD TCPIP
BIND IP TO TOKEN-IP ADDR=129.33.160.161
     MASK=255.255.255.0 GATE=129.33.160.254
LOAD ROUTE
LOAD TSA410
LOAD TSANDS
```

Figure 36. Sample TCPRECOV.NCF File: NetWare 4.10

- **Add NetWare files**

  Copy the following NetWare files to disk 2:

  ```
  AFTER311.NLM
  CSLSTUB.NLM
  EDIT.NLM
  INSTALL.NLM
  IPXS.NLM
  MSM.NLM
  NWSNUT.NLM
  ROUTE.NLM
  SMDR.NLM
  SNMP.NLM
  SPXS.NLM
  TCPIP.NLM
  TIMESYNC.NLM
  TLI.NLM
  TOKENTSM.NLM
  ```

Copy any name space module used, for example, MAC.NAM.

If you run out of space, copy the remainder to a third formatted diskette (Disk 3).

Create Disk 3

- Format another 1.44 MB diskette, label it as INSTALL, and mark it disk 3.

  This diskette is required to rebuild the NetWare 4.10 NDS from bare metal. The layout of the subdirectories on this diskette is important.

- **Add NetWare files**

  Copy the following NetWare files to disk 3:

  ```
  NETMAIN.ILS
  CLIB.NLM
  DS.NLM
  DSAPI.NLM
  DSI.NLM
  ICMD.NLM
  MATHLIBC.NLM
  STREAMS.NLM
  TSA410.NLM
  TSANDS.NLM
  ```

- Create subdirectory A:\BOOT\NATIVE on disk 3 and copy NETMAIN.ICS to this subdirectory.
- Create subdirectory A:\SCRIPTS on disk 3 and copy LANGFS.ILS to it.
- Create subdirectory A:\LOGIN\NLS. on disk 3 and move in the basic unicode files used on the NetWare server.

  There are four basic unicode files. For a DOS environment using codepage 437 and U.S. English, they are:

  ```
  UNI_437.001 (Translates from Unicode to US English)
  437_UNI.001 (Translates from US English to Unicode)
  UNI_MON.001 (For monocasing the Unicode for comparison)
  UNI_COL.001 (Allows the Unicode to be sorted or collated)
  ```

Note: After you have successfully tested the diskettes created, you may use any available zipping tool to save diskette space or even to create self-installing extract diskettes. The additional steps involved are not discussed here.

Create Copy of ADSM Client Diskettes: Use the DOS DISKCOPY command or any other DOS utility to make a duplicate copy of the ADSM NetWare client installation diskettes.

The License Diskette: The original Novell NetWare 4.10 license diskette for this server has to be available during the recovery.

12.3 Using Bootable Diskettes: Postdisaster Recovery

In this section we describe how to recover a Novell NetWare Version 4.10 server from a disaster using the information you saved before the disaster (described in 12.2, “Bare Metal Recovery With Bootable Diskettes: Predisaster Preparation” on page 196) and the bootable diskettes you created (described in 12.2.2, “Creating the Bootable Diskettes” on page 199).

12.3.1 Rebuild the Hardware Environment

Retrieve information about the Novell NetWare server machine to help re-create the hardware environment of the destroyed ADSM client.

If you used DRM as the repository for information about the Novell NetWare server machine, retrieve it by issuing the appropriate ADSM queries to the ADSM server. For examples of these queries, see 1.3.6, “Disaster Recovery Manager” on page 18.

12.3.2 Boot the Recovery System

The recovery procedure described here applies only to a NetWare Version 4.10 server in a single-server environment.

Use the NetWare Version 4.10 bootable diskettes to boot the replacement hardware and prepare for ADSM file recovery. Follow the steps listed below.

Note: We made the assumption that all NetWare-related files on the C: drive are stored in a directory other than the root directory. We used C:\SERVER.410 as our directory.

12.3.2.1 Step 1: Boot the New Machine from Disk 1

Boot the new machine from disk 1.

12.3.2.2 Step 2: Create a Small DOS Partition

If there is already a small DOS partition on the first drive and its size is adequate, you can skip this step. Do not use an unnecessarily large size for the DOS partition. Set aside enough free space for the NetWare partition.

Run the DOS FDISK command to create a DOS partition on the (first) drive. Use the size you recorded before the disaster. Once you have changed the partition, you have to reboot the machine when you exit FDISK. Leave disk 1 in the diskette drive.

12.3.2.3 Step 3: Create a Bootable DOS Partition (C: Drive)

If the DOS partition is already bootable or formatted, you may not want to reformat it. However, DOS modules are version sensitive, so we recommend that you transfer the DOS system files from disk 1 to the C: drive. To transfer the files, issue this command:

```
SYS C:
```

Transferring ensures that both the DOS system on the C: drive and those DOS files to be copied over later are at the same level.

If the DOS partition has just been created, format it with the /S and /V options:

```
FORMAT C: /S/V
```

/V is optional. If used, you are prompted to specify a label for the drive at the end of the formatting. You may, however, choose not to provide a label. You can also use the LABEL command to change the label of a drive at any time. The command syntax is:

```
LABEL C:
```

12.3.2.4 Step 4: Copy Files on Disk 1 to the C: Drive

If you want to put all NetWare files on the C:drive′s root directory, issue the COPY command:

```
COPY A:*.* C:\
```

and go to Step 5.

Otherwise, put all NetWare files on the C:\SERVER.410 directory. To create this directory and make it the current directory, issue these commands:

```
MD C:\SERVER.410

CD C:\SERVER.410
```

Copy all NetWare files from disk 1 to this directory, that is, move all files with extensions of LAN, DSK, NCF, or NLM. Copy SERVER.EXE to disk 1. For example:

```
COPY A:TOKEN.LAN  C:
```

Copy the DOS files (including CONFIG.SYS and AUTOEXEC.BAT) to the root directory. You can use a wild card for the group copying:

```
COPY A:*.COM C:\
```

12.3.2.5 Step 5: Copy Files on Disks 2 and 3 onto the C: Drive

To copy the contents of disk 2 to the current directory of the C: drive, issue this command:

```
COPY A:*.*  C:
```

Copy only the NLMs on disk 3 to the C: drive:

```
COPY A:\*.NLM  C:
```

If you used additional diskettes to hold the NLM files, remember to copy them to the C: drive.

12.3.2.6 Step 6: Modify the CONFIG.SYS and AUTOEXEC.BAT Files

If CONFIG.SYS exists and is copied, make sure the path statements in it are changed to point to the C: drive instead of A: (the diskette drive). Use the EDIT command to modify the file:

```
EDIT C:\CONFIG.SYS
```

Do the same for the AUTOEXEC.BAT file. This is also a good time to comment out the unnecessary statements in these files. Make sure the AUTOEXEC.BAT does not load the SERVER.EXE.

12.3.2.7 Step 7: Reboot the System from the C: Drive

Remove any diskette in the diskette drive and reboot the system. The machine should come up as when you booted it with disk 1, except with the C:> prompt displayed instead.

12.3.2.8 Step 8: Load NetWare Kernel SERVER.EXE

If you have put all NetWare files in a particular directory, set it as the current directory:

```
CD \SERVER.410
```

Start the server without loading the AUTOEXEC.NCF file; use this command:

```
SERVER -NA
```

You are asked to specify the Server's Name and the Server's IPX internal network number. Respond with the information you recorded for this server before the disaster.

12.3.2.9 Step 9: Create the NetWare Partitions

Load the NetWare installation utility (INSTALL.NLM) from the server console:

```
LOAD INSTALL
```

From the **Installation Options** menu, select **Disk Options**.

From the Available Disk Options menu, select **Modify disk partitions** and **Hot Fix**.

If NetWare detects more than one hard disk, it displays the Available Disk Drives panel. Select the drive you want to create the first NetWare partition.

Note: The first partition need not be on the first physical drive. If you do not see as many disk drives as you expect, the most likely explanation is that all of the required NetWare disk drivers have not been loaded.

Two panels are displayed. One, as background, shows partition information, for example, types and sizes of the partitions that have already been defined and free space information. (If a NetWare partition has been defined, or no more free space is available on this drive, you will not be able to define one.)

On the other panel (Disk Partition Options) you can create or delete a NetWare partition. Select **Create NetWare disk partition**.

On the **Disk Partition Information** panel, you can specify the partition size by cylinder or by capacity. Refer to the information you have recorded for this server before the disaster.

You can change the Hot Fix value or leave it as is.

Press <ESC> and reply YES to create the partition.

Do the same to create other partitions for this server.

12.3.2.10 Step 10: Create the NetWare Volumes

From the Installation Options menu, select **Volume options**.

The Volume Name/Size menu displayed will have a blank entry because a NetWare volume has not been defined at this stage.

Press <INSERT> to create new volume. The Volume Disk Segment List panel displays the device number and free space information. Move the cursor to highlight a device (drive) that contains free space and press <ENTER>.

On the next panel (Disk Segment Parameters) you can define the name and size of a volume. NetWare always defaults the first volume defined to SYS. It also always assumes that you want to use all of the free space when you define a volume. Refer to the information you recorded for this server before the disaster and specify the **Disk segment volume name** and **Disk segment size**.

Press <ESC> to return. The Volume Disk Segment List panel will be updated with the new definition. The information, however, is not really saved at this point.

Do the same to create all other volumes for the server. You must create the volume before starting the ADSM restoration for a volume.

Before you leave the Volume Name/Size menu, you are prompted to save the changes. Reply <YES>.

After formatting the volumes, NetWare prompts you for an action. Select **Mount all volumes**.

After NetWare has mounted the SYS volume, it attempts to load the DS NLM from SYS:\SYSTEM. It will, of course, fail because SYS:\SYSTEM is still empty. This information is reflected on the server console.

12.3.2.11 Step 11: Add DOS Paths to the Server's Search Path

Once NetWare has mounted the SYS volume, it will change its search path to SYS:\SYSTEM. You can display the NetWare search path any time by issuing the SEARCH command from the server console. If you are currently not at the console screen, switch to that screen either by toggling around (use <ALT>+<ESC>) or select directly after pressing <CTRL>+<ESC>.

Add the DOS directory where the NetWare files are kept to the search path:

```
SEARCH ADD C:\SERVER.410
```

or

```
SEARCH ADD C:\
```

Add a search path to point to the diskette drive:

```
SEARCH ADD A:\
```

12.3.2.12 Step 12: Load the DS NLM

From the server console, enter:

```
LOAD DS
```

DS will be loaded successfully but the NDS will issue this message: *Could not open local database*.

12.3.2.13 Step 13: Install the Server License

Note: You may choose to install the server license at a later stage.

Insert the Novell NetWare 4.10 license diskette for this server into the diskette drive.

Load the INSTALL NLM from the server console, if it is not already loaded.

From the Installation Options panel, select **License option**.

After installation, the license information is displayed on the server console.

12.3.2.14 Step 14: Install NetWare Files from Disk 3

Insert disk 3 into the diskette drive.

Load the INSTALL NLM from the server console, if it is not already loaded.

From the Installation Options panel, select **Copy files option** and choose the default path (A:\).

After initial file copying from disk 3, you are prompted to specify a server boot path. Use the DOS search path where the SERVER.EXE is kept, for example, C:\SERVER.410.

On the next panel (Indicate Which File Groups You Want Installed) you can install NetWare files by group. Uncheck ALL groups except the **Pre-install Files**. Press <F10> to continue.

You can expect to receive error messages when NetWare tries to copy files from the following subdirectories:

```
A:\SYSTEM\PREINST\*.*
A:\LANDRV\CORE\*.*
A:\DISKDRV\CORE\*.*
A:\LOGIN\*.*
A:\LOGIN\DOS\*.*
A:\LOGIN\OS2\*.*
```

For each case, press <ENTER> to get to the next panel. Choose **Continue copying the next file** to continue.

When all files on disk 3 are installed, you are returned to the Installation Options panel.

12.3.2.15 Step 15: Install the NetWare Directory Services

From the Installation Options panel, select **Directory options**.

Choose **Install Directory Services onto this server** from the Directory Services Options panel.

The next message panel displayed is informational. Press <ENTER>, then reply <Yes> to continue.

Select **Yes, this is the first NetWare 4 server**.

Enter the directory tree name for this server, for example, ITSC410A.

Select a Time Zone. Fill up the time configuration parameters and press <F10> to save the information.

On the next panel (Context For This Server) you can specify the server context and the administrator's password. You will be asked to verify the password entered.

Reply <Yes> to save the directory information.

After installing the NDS, NetWare redisplays the information you have just specified. It also issues the following informational messages on the server console:

- Bindery open requested by the SERVER
- Established communication with server ......
- Directory Services: Local database is open

The base schema will be available when NDS is first created. If the server had a vendor product installed to extend the schema, you have to reinstall the product before restoring the NDS.

12.3.2.16 Step 16: Run the TCPRECOV NCF

If you have to review or modify the contents of the TCPRECOV file, load the NetWare EDIT NLM from the server console to do so.

Issue the TCPRECOV command from the server console:

```
TCPRECOV
```

Note: If a name space other than DOS is used, you can add the required name space support (using server console command ADD NAME SPACE) at this time. For example:

```
ADD NAME SPACE MAC TO SYS
```

You can check and verify the status of the TCP/IP network by issuing the NetWare server CONFIG command.

12.3.2.17 Step 17: Install the ADSM NetWare Client

Insert the ADSM NetWare Client Installation diskette into the A: drive.

From the server console, enter:

```
LOAD  A:\INSTDSM
```

There are three installation options. You do not have to install the API code at this time. Installation of SMS Modules is optional as the NLMs were also copied to disks 2 and 3. The sequence of installing ADSM and SMS Modules is immaterial.

You are prompted to specify the target directory for both cases. For the ADSM client code, you can define the target directory of your choice. For the SMS modules, we recommend that you use the default directory, SYS:\SYSTEM. We used the default directory for both cases.

After installation, add the new paths to NetWare's search path:

```
SEARCH  ADD   new_directory
```

We chose to add the search path (SYS:\ADSM) in the TCPRECOV.NCF file.

12.3.2.18 Step 18: Create the ADSM NetWare Client Options File

Load the EDIT NLM from the server console:

```
LOAD  EDIT
```

In the File To Edit window, enter:

```
SYS:\ADSM\DSM.OPT
```

(or use the path of your choice).

Reply YES to create.

On the blank screen, type in the following values for your server setup:

```
NODENAME           ADSM_nodename_for_this_client
COMMMETHOD         TCPIP
TCPSERVERADDRESS   the_ADSM_server_IP_address
TCPPORT            the_ADSM_server_TCPIP_port
```

For example, the DSM.OPT we used looked like this:

```
NODENAME            ITSC410A
COMMMETHOD          TCPIP
TCPSERVERADDRESS    129.33.160.100
TCPPROT             1500
```

Press <ESC> and reply YES to save this file.

12.3.2.19 Step 19: Start the ADSM NetWare Client Application

From the server console, issue:

```
LOAD DSMC
```

When the ADSM application is successfully loaded, the **DSMC>** prompt will be displayed and you are ready to issue ADSM client commands.

12.3.2.20 Step 20: Rebuild the NetWare Server

You are now ready to start file restoration, using ADSM. To check the active backups stored at the ADSM server for this client, enter the following at the **ADSM>** prompt:

```
QUERY  VOLUME
```

You are prompted to provide the password for the node name specified in the DSM.OPT file. You must provide the correct password to be able to proceed further. If the correct password is not part of the information recorded before the disaster, the ADSM administrator can change the ADSM node password.

The active volume backups, including the directory, will be displayed.

The first file to restore is the directory. Issue this command:

```
RESTORE  ITSC410A\DIRECTORY:  -REPLACE=YES
```

You are asked to enter the NetWare user for this node. Reply ***admin*** and enter the password you set earlier for this administrator user.

If you do not specify the ***REPLACE*** option, you are prompted to either replace or not replace the current directory. Reply YES.

After the directory has been successfully restored, rebuild the SYS volume:

```
RESTORE ITSC410A\SYS:* -REPLACE=YES -SUBDIR=YES -VOLINFORMATION
```

Note: ADSM cannot overwrite files that it uses. When prompted, select **skip** to continue the restoration process.

Restore any other NetWare volumes, using the same command. Replace the SYS with the respective volume name, for example, APPL, VOL1.

12.3.2.21 Step 21: Restart the Server

You are now ready to restart the recovered Novell NetWare 4.10 server. Before you shut down the server, first verify that the restored AUTOEXEC.NCF file correctly describes your current machine setup (for example, check the disk and LAN drivers, and the slot-number used).

There are at least two ways to edit the AUTOEXEC.NCF file on the SYS:\SYSTEM directory. Either use the NetWare EDIT module as described earlier or go through the Installation Options panel, NCF files options, and select the Edit AUTOEXEC.NCF file.

From the server console, enter: DOWN. After the server is shut down, type EXIT to return the machine to DOS.

At this point you may want to restore the original CONFIG.SYS and AUTOEXEC.BAT files by uncommenting all lines you commented out when you prepared the bootable diskettes. You may also want to reinsert the SERVER.EXE statement in the AUTOEXEC.BAT file so that the NetWare server will be started automatically.

Restart the server, using your normal procedure.

Login as administrator to verify the file system and trustee assignments.

You may also want to run the DSREPAIR utility to ensure that the restored NDS is at a consistent state. Refer to NetWare 4.10 documentation if you need more information regarding DSREPAIR utility.

If you had files and programs stored on the base, bootup, C: DOS partition and you kept a separate backup of these files, you can restore them now. You have to shut down the server and return to DOS.

At this point, you may also want to reinstall the updates or PTFs for the ADSM NetWare Client.

12.4 Recovery with Bootable Diskettes/ADSM Peer

In the previous section we outlined the steps to recover a Novell NetWare Version 4.10 server to the point where it could begin the ADSM client restore using TCP/IP communications to the ADSM server.

In this section we talk about an alternative method to perform ADSM restore when there is no direct TCP/IP link between the destroyed NetWare ADSM client and its ADSM server. This may be the case where SNA LU6.2 was used or there is no direct communication link between the ADSM client and the server.

NetWare servers are normally linked together and capable of exchanging data among themselves through the NetWare's SMS interface using the IPX/SPX communication protocol. ADSM takes advantage of the feature and supports this capability of NetWare's SMS. A NetWare ADSM client can therefore perform ADSM backup/restore services on behalf of its logically linked peer, which may or may not have a direct connection to the ADSM server (see Figure 37). In other words, as long as the link between the gateway NetWare Client and the ADSM server is not broken, it is always possible to recover a crashed NetWare server regardless of whether a direct communication link is available.

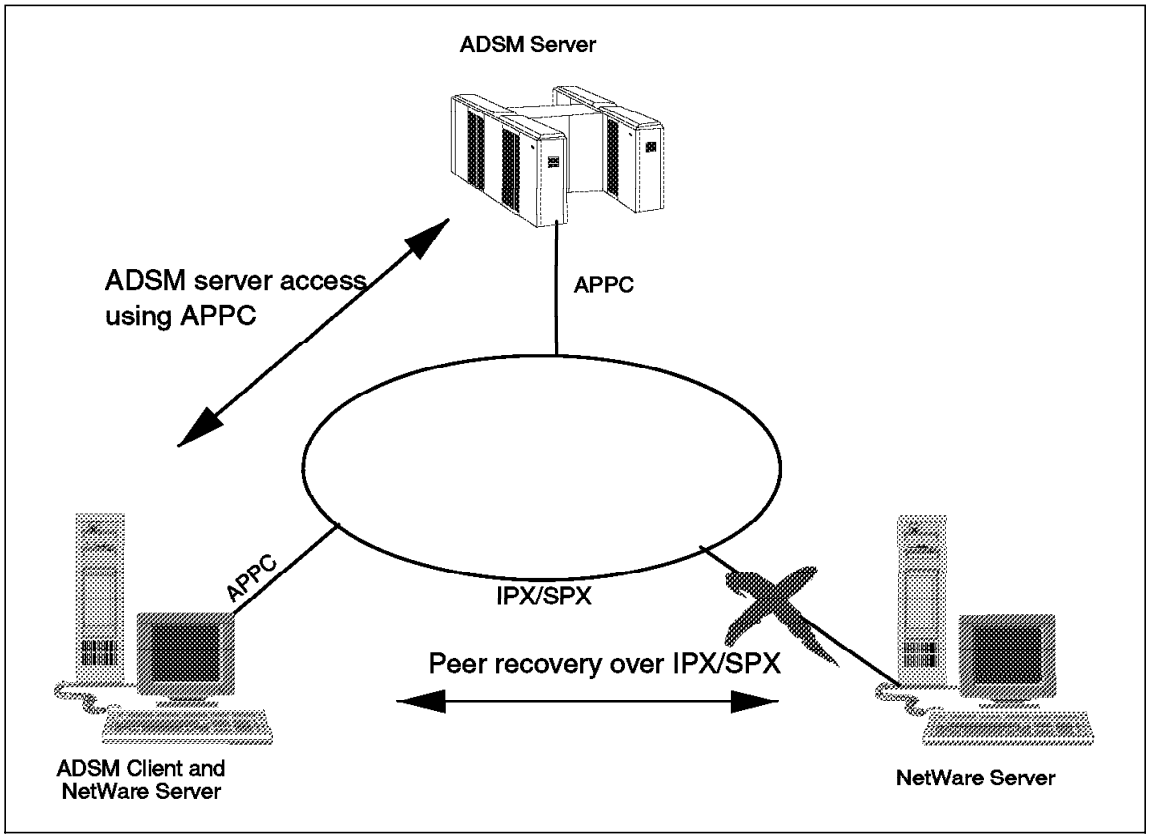


Figure 37. Using a Peer NetWare 4.10 Server to Perform Proxy ADSM Recovery

Note: Of course, a direct connection between the ADSM client and server is always preferable from a network and server performance standpoint. So you would only use this method if you had no alternative in a disaster recovery situation.

12.4.1 Predisaster Preparation: Peer Recovery

The information we recommend you save before the disaster for this method is the same as that described in 12.2, “Bare Metal Recovery With Bootable Diskettes: Predisaster Preparation” on page 196 with the following exceptions:

Add

Because you will be using IPX instead of TCP/IP to facilitate the ADSM restore, you have to save the *IPX external network number* used when joining the physical network. (Note: This is different from the *IPX internal network number*.) You can obtain this information from the AUTOEXEC.NCF file or by using the CONFIG server command and looking under ***LAN protocol : IPX network...*** Add this information to the other data you are saving in preparation for disaster.

After you use the bootable diskettes and the proxy ADSM recovery by a peer Novell NetWare server, the assumption is that you will want to reestablish communications between the restored ADSM client and the ADSM server. So record any specific information (for example, for an SNA LU 6.2 implementation) your installation will require.

- **Delete**

  Because you will be using IPX instead of TCP/IP and depending on a peer Novell NetWare server for its ADSM client, information related to the use of TCP/IP and ADSM is not required (though it certainly does not hurt to record it anyway).

12.4.1.1 Authorize a Peer Novell NetWare Server ADSM Client

Before the disaster, you must authorize the peer Novell NetWare ADSM client to restore your ADSM backups. For example, if one Novell NetWare ADSM client, **NW410A**, wants another Novell NetWare ADSM client, **NW410B**, to have the authorization to restore his backups, he would use the following ADSM command:

```
SET ACCESS BACKUP * NW410B
```

If ADSM client NW410B wants to check who has been authorized to restore his backups, he would use the following ADSM command:

```
QUERY  ACCESS
```

12.4.1.2 Create the NetWare Bootable Diskettes

Create the NetWare bootable diskettes, using the procedure outlined in 12.2.2, “Creating the Bootable Diskettes” on page 199, with the following differences:

Optional: If you want, you can make the following modifications (though if you do not, these elements just will not be used):

- ADSM client installation diskettes not required

  Because you are depending on a peer Novell NetWare ADSM client to perform the ADSM restore on our behalf, you can choose not to include the copies of the ADSM NetWare client installation diskettes.

- These NLMs no longer required

  For the same reason, the following NLMs need not be copied to disk 2 of the bootable diskettes:

  ```
  TCPIP
  SNMP
  IPXS
  MATHLIBC
  ```

Mandatory: The TCPRECOV.NCF file (see Figure 36 on page 202) is valid for using a TCP/IP connection only. Modify this file to reflect the IPX communications you intend to use to communicate with the peer Novell NetWare server. To eliminate confusion, we rename this file to

`IPXRECOV.NCF`

. Figure 38 shows the contents of a sample file.

```
LOAD CLIB
LOAD DSAPI
LOAD TOKEN NAME=TOKEN-IPX
BIND IPX TO TOKEN-IPX NET=00000002
LOAD ROUTE
LOAD TSA410
LOAD TSANDS
```

Figure 38. Sample IPXRECOV.NCF File: NetWare 4.10

12.5 Postdisaster Recovery Using Peer Recovery

The steps to do bootable diskette recovery with an ADSM Peer Novell NetWare server is very much like those described in 12.3, “Using Bootable

Diskettes: Postdisaster Recovery" on page 204. Follow these steps until NDS is installed and the local database is open.

The base schema will be available when NDS is first created. If the server had a vendor product installed to extend the schema, you have to reinstall the product before restoring the NDS.

Next, bring up the IPX/SPX network. We prepared the necessary commands in our IPXRECOV.NCF file (see Figure 38 on page 216.). If you have to edit this file, use the NetWare EDIT command. To start the network, issue the IPXRECOV command from the server console.

To check the network status, use the CONFIG server command.

Once the communication between the peer NetWare servers is up, you are ready to restore the files to the new (target) server.

Start the ADSM client on the peer NetWare Server.

From the

```
ADSM>
```

prompt, issue the ADSM command to restore the directory on behalf of this target server. (We called the target server NW410A).

```
RESTORE -FROMNODE=NW410A NW410A\DIRECTORY: -REPLACE=YES
```

After entering this command, you are prompted for the ADSM password to start a session with the ADSM server.

Depending on the NWPWFILE setting in the DSM.OPT file on this server, you are prompted to enter the NetWare user of the **target** server. Use **admin** and provide the password you have just set up.

After the directory is restored, rebuild the SYS volume:

```
RESTORE -FROMNODE=NW410A NW410A\SYS: -REPLACE=YES -SUBDIR=YES
        -VOLINFORMATION
```

Note: ADSM cannot overwrite some of the unicode files that are in use. When prompted, select **skip** to continue the restoration process.

Continue to restore other volumes in the same way.

Before restarting the new server, you may want to first modify the AUTOEXEC.NCF file. Use the NetWare EDIT NLM or access this file through the Installation Options panel.

Shut down the recovered server and exit to DOS (enter **DOWN** and then **EXIT** from the console).

At this point you may want to restore the original CONFIG.SYS and AUTOEXEC.BAT files used. You may also want to reinsert the SERVER.EXE statement in the AUTOEXEC.BAT file so that the NetWare server will be started automatically.

Restart the server, using your normal procedure, and login as administrator to verify the file system and trustee assignments.

You may also want to run the DSREPAIR utility to ensure that the restored NDS is at a consistent state. Refer to NetWare 4.10 documentation if you need more information regarding DSREPAIR utility.

If you had files and programs stored on the C: DOS partition, which was outside the scope of the backups we discuss here, but for which you may have kept a separate backup, you may restore them now. You will have to shut down the server and return to DOS to do so.

At this point, you may also want to reinstall the updates or PTFs for the ADSM NetWare Client.

Chapter 13. AIX Version 3.2.5 Recovery

In this chapter we discuss using the MKSYSB utility to recover an AIX Version 3.2.5 client environment that uses TCP/IP to communicate with its ADSM server.

We cover the kind of information that should be backed up before the disaster, how to prepare for the MKSYSB, and how to use these to recover an AIX Version 3.2.5 environment after a disaster.

13.1 Product Overview

AIX Version 3.2.5 is IBM′s implementation of the UNIX operating system. AIX is typically used in medium- to large-scale environments and is a full 32-bit multitasking, multiuser operating system. To understand the issues involved in AIX client recovery, you must first understand some of the specific areas of the AIX Version 3.2.5 operating system.

AIX Version 3.2.5 runs exclusively on the wide range of IBM RISC System computers (RS/6000). RS/6000s range from small, desktop, uniprocessor machines of both microchannel architecture (MCA) and personal computer interface (PCI) design to symmetric multiprocessor (SMP) machines and large-scale parallel systems. AIX Version 3.2.5 can be used on all RS/6000 platforms except SMP and PCI-based machines.

For a more detailed discussion of the AIX Version 3.2.5 operating system, see *AIX Version 3.2 System Management Tips and Techniques* (GG24-4161-00).

13.1.1 Storage

Storage media used in AIX Version 3.2.5 include tape, CD-ROM, and disk. Disk storage is handled by the logical volume manager (LVM), which stores the data on the disk using the journaled file system (JFS). The LVM makes boundaries between physical disk volumes (PVs) transparent to the user and the system through logical volumes (LVs). Each LV contains a JFS file system (see Figure 34 on page 191).

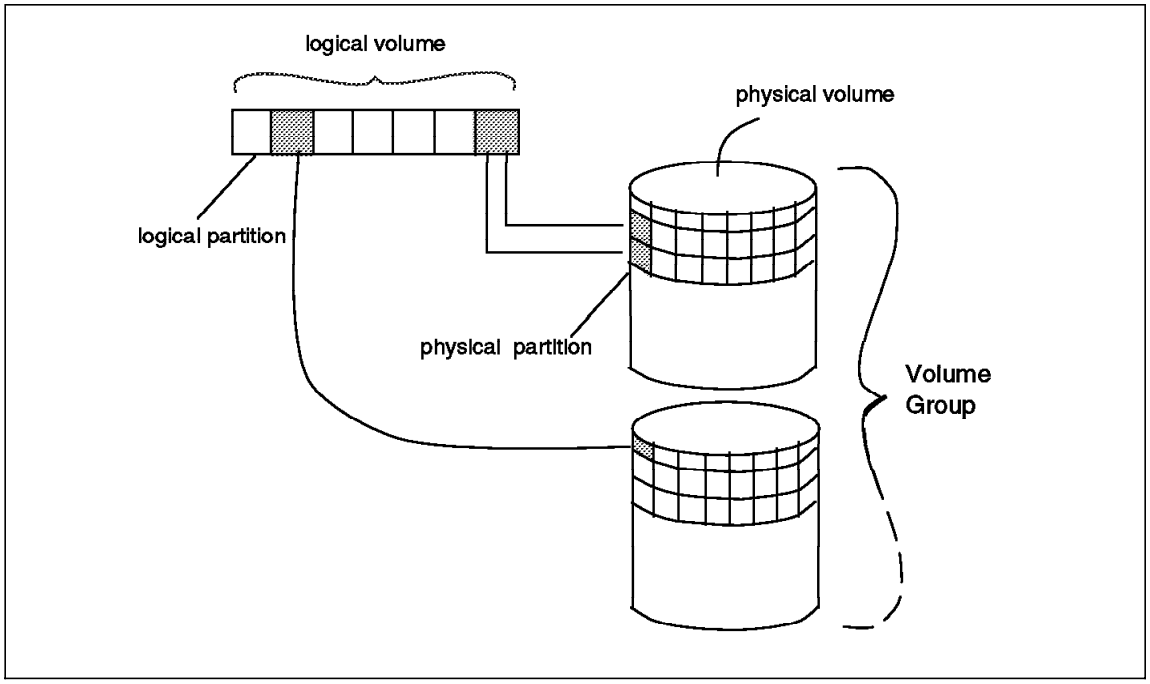


Figure 39. AIX Logical and Physical Storage

PVS can be grouped together in volume groups (VGs), each VG consisting of one or more PVs. The AIX Version 3.2.5 operating system files typically occupy the primary or root VG (rootvg). File system security in AIX Version 3.2.5 is handled by means of file permissions, which dictate whether another user can read, write, or execute a file on the system. This method can be further enhanced by the use of ACLs to define file permissions on a per-user level.

13.1.2 System Backup

The most effective way of backing up the AIX Version 3.2.5 operating system is with the `mksysb` utility. This is not what most people would consider a normal backup, but it is a more dynamic system backup. During a mksysb restore, certain system files, such as the object data manager (ODM) and device files, in the */dev* directory are reconfigured to match the system to which mksysb is being restored. Thus the mksysb backup can be restored onto systems that are of a different configuration than the original. This approach has its limits and is supported only between machines of a similar configuration, but it is possible between most machines in the RS/6000 range.

13.2 Predisaster Preparation

The disaster we are preparing for is the total and catastrophic loss of the ADSM client, where provision has to be made to restore everything from the bare metal up. If our disaster recovery preparations can cover this worst case scenario we can assume that they will also be able to handle recovery from lesser disasters.

In this section we discuss the information to collect and save before a disaster to enable a bare metal restore.

13.2.1 ADSM Backup

An AIX Version 3.2.5 mksysb includes all mounted file systems in the rootvg, so it is necessary to ensure that the ADSM backups contain all data not in this category.

The method we discuss here was tested on a machine where only the base operating system was stored in rootvg and all other files were mounted in external volume groups. Thus we were able to use the default exclude list for all UNIX systems included with the ADSM distribution, with only the root smit.script, usually found in the root directory, defined as extra.

We set the copy group to use shared static option to avoid fuzzy backups.

For more information about AIX Version 3.2.5 systems that have space-managed file systems, see *Using ADSM Hierarchical Storage Management*, SG24-4605-00.

13.2.2 Operating Environment of the ADSM Client

In preparation for disaster recovery we recommend that you collect and save offsite the information listed below in addition to the ADSM backup data. Depending on your installation, you could save this information by using the DRM feature, or you could save it on hardcopy stored offsite. The way in which you save the information is not as important as ensuring that it is saved **somewhere** where it can be easily retrieved along with the client recovery media when a disaster occurs.

- **Hardware configuration**

  Use the `uname -m` command to collect information about the machine type. This will return a 13-digit code of the form xxyyyyyymmss, where xx is always zero and indicates the system, yyyyyy indicates a unique identification number for the whole system, mm indicates a two-character code for the machine type, and ss indicates the sub-model number and should always be zero. Information about the installed hardware in the machine is included in output from the `lscfg -v`

command. The output lists all adapters in the machine and specific information about their model, make, and microcode level where appropriate.

- **Logical storage information**

  Information regarding the storage setup of the client machine is vital to system recovery. The size of all disks in each VG, the number of LVs in each VG, and the size of each LV should be stored before the disaster in either hardcopy or within DRM.

  To list the physical disks per VG, issue this command:

  `lsvg -p` *vgname*

  To list the LVs per VG, issue this command:

  `lsvg -o | lsvg -i -l`

  To list details about each LV, issue this command:

  `lslv` *lvname*

  Note:

  The AIX Version 3.2.5 mksysb utility does not cater for LV placement information. If you have tuned your system′s performance in this way, it will have to be retuned after the restore. To show information about the placement of each LV on the physical disks, issue:

  `lslv -l lvname`

  The mksysb utility cannot store any ACLs on the system, and paging space definitions are reset at restore time.

  For information about dealing with these and any other mksysb issues, contact your local IBM support representative and see 13.3.2.4, “Other Methods” on page 232.

- **Communications details**

  The information necessary to document your communications setup will depend on which protocol you are using. For TCP/IP note such items as the internet address, host name, default gateway, and netmask. For more detailed information take a copy of the output from:

  `lsattr -l` *adapter name* `-E`

  For example, this command will produce the output shown below:

  `lsattr -l tr0 -E`

```
mtu       1492           Maximum IP Packet Size for This Device     True
mtu_4     1492           Maximum IP Packet Size for This Device     True
mtu_16    1492           Maximum IP Packet Size for This Device     True
remmtu    576            Maximum IP Packet Size for REMOTE Networks True
netadddr  129.33.160.145 Internet Address                           True
state     up             Current Interface Status                   True
arp       on             Address Resolution Protocol (ARP)          True
allcast   on             Confine Broadcast to Local Token-Ring      True
hwloop    off            Enable Hardware Loopback Mode              True
netmask   255.255.255.0  Subnet Mask                                True
security  none           Security Level                             True
authority                Authorized Users                           True
broadcast                Broadcast Address                          True
```

Note:

You can collect all of the above information and store it in a single file. Construct a shell script that will collect the information about each item and then add it to a specified file either for inclusion into the DRM or for backup and restore after a disaster.

For example, this shell script gathers information about the details and physical placement of each LV on the system:

```
for i in lsvg do
        for j in lsvg -l $i | cut -d" " -f1
        do
            echo "$i/$j:\n"
            echo "Details:"
            lslv $j 2> /dev/null
            echo "\nLocations:"
            lslv -l $j 2> /dev/null
            echo "\n"
            echo "═══════════════════════════════════════════════════"
        done done
```

If you make this script executable and run it with:

```
./script >> /tmp/sys_info
```

it will append (>>) the information to the end of the /tmp/sys_info file.

To enter the name and location of this file into the recovery information entry for that machine's definition in DRM, issue this command:

```
adsm> insert machine machinename sequencenumber \
recoveryinstructions="Machine Configuration Stored in /tmp/sys_info"
```

Optional: Statistics for Postdisaster Recovery Verification

You may want to collect and save information that you can use after a disaster once the restore process is complete to validate that all information has indeed been restored correctly. Each installation will have its own ideas about the best way to verify that the recovery is complete. Some possible sources of information for this type of verification are:

- Information about installed software (`lslpp -Al`)
- Size of data files (`ls -al`)

13.2.3 Creating the Bootable Mksysb Tape

In this section we describe a method to create a bootable tape for AIX Version 3.2.5. We also discuss some AIX system backup issues and some common problems that occur when creating a mksysb.

13.2.3.1 Assumptions

These instructions apply to any AIX Version 3.2.5 system using ADSM.

The instructions apply to the following products:

- AIX Version 3.2.5
- ADSM/AIX Version 1, Release 2 client code
- ADSM/AIX Version 2, Release 1 client code
- Any ADSM server that uses TCP/IP

A complete ADSM backup as described in 13.2, “Predisaster Preparation” on page 221 should be available at the ADSM server, and the restore should be done to a hardware configuration similar to that of the original ADSM backup/archive client machine.

13.2.3.2 Configuration Used to Test This Technique

We tested this technique, using the following configuration:

- RISC System/6000 7013-320H with 128 MB of RAM
- IBM High-Performance Token-Ring Adapter (093F1277)
- Four 1 GB and two 400 MB SCSI-attached disk drives
- AIX Version 3.2.5
- ADSM/AIX Version 2, Release 1, Level 3 client code
- ADSM/AIX Version 2, Release 1, Level 9 server code

To use this technique you will need:

- Internal or external direct-attached tape drive
- One blank data grade tape

13.2.3.3 Step-by-Step Instructions

For these tests we decided to store all *system data* in a mksysb image and all *user data* with ADSM. We defined system data as operating system essential files and user data as all user data files and application files. This enabled us to limit the time required to back up and restore the base system while allowing users the advantages of conventional ADSM backup and restore.

We also be used the smit.script file to act as a system change log and a quick method of recovering the system to a point-in-time configuration. By zeroing in the smit.script file for root after each mksysb backup, as long as all CONFIG changes are done through the System Management Interface Tool, SMIT (as root), the `smit.script` could be run after a restore to restore the system to its latest configuration.

Step 1: Preparing the System for Mksysb

Decide on a suitable time for the mksysb image to be taken of the system. The time is best when there is as little user activity as possible. Although user activity should not be able to compromise the integrity of the mksysb, system performance will be hit severely during the backup.

To ensure that the tape drive you intend to use is defined to the system and available for use, issue this command:

```
lsdev -Cc tape
```

This should produce output similar to the following:

```
rmt0 Available 00-08-00-3,0 2.3 GB 8mm Tape Drive
```

Use the `df` command to check which file systems are mounted and unmount any non-system-data file systems, using the `unmount` command. The only file systems that should be included in the `df` output should be these:

```
Filesystem    Total KB    free %used   iused %iused Mounted on
/dev/hd4       16384       88   99%     859    20%  /
/dev/hd9var    12288     6148   49%     185     6%  /var
/dev/hd2       962560  524496   45%   12787     5%  /usr
/dev/hd3       24576     7948   67%     227     3%  /tmp
```

The system is now ready to be backed up.

Step 2: Backing Up the System with Mksysb

First build the .fs.size file, which stores information about the sizes of the file systems for re-creation at restore time. It is vital that this be done before a mksysb is taken of your system. Use the mkszfile command to create a mksysb:

```
mkszfile&&mksysb /dev/rmtX.1
```

where && indicates that the second command, the mksysb, should be started only if the mkszfile command completes successfully.

Note:

The mkszfile may fail if fewer than 500 blocks are free in any of the file systems. Check this by looking at the output of the df command and the Free column for each file system.

The X refers to the number of the tape drive you want to use, and the .1 indicates that the tape should not be rewound after each end of file marker.

Note:

A bootable mksysb tape is actually made up of four images: the first is the bootable image: the second, the maintenance image; the third, a dummy table of contents; and the fourth, the actual data stored as a tar archive. Without the .1 extension on the tape drive name, each image would overwrite the subsequent images, and the tape would no longer be bootable.

The mksysb command can also be run through SMIT with a fastpath of either smit startup or smit mksysb. This will automatically run the mkszfile command before backing up and will provide the .1 onto the tape drive name. The smit mksysb screen is shown below.

```
                              Backup the System

Type or select values in entry fields.
Press Enter AFTER making all desired changes.


                                                      ·Entry Fields“
    WARNING:  Execution of the backup command will
              result in the loss of all material
              previously stored on the selected
              output medium. This command backs
              up only rootvg volume group.

  FORCE increase of work space if needed              no               +
* Backup DEVICE or FILE                              ( )
    (example: /dev/rfd0)




F1=Help             F2=Refresh          F3=Cancel           F4=List
F5=Reset            F6=Command          F7=Edit             F8=Image
F9=Shell            F10=Exit            Enter=Do
```

Once the appropriate information is input to SMIT, the mkszfile and mksysb commands will be run and the system backup will be made.

After the backup has completed, remount the file systems that you unmounted before the backup and zero the smit.script file on the root directory, using this command:

```
>/smit.script
```

If you changed the default home directory of the root user, this smit.script file will be stored in that directory instead of the root directory.

Note:

If you want to automate this process, zero the smit.script file, do all the above tasks, and then set the resulting smit.script file to be run by the AIX cron utility at regular intervals.

Step 3: Backing Up User Data with ADSM

You must now back up any user data on the system that was not in the file systems backed up by the mksysb. Include the /home file system, any file systems in the rootvg that you created manually, and all file systems in external VGs. The regularity with which you back up this data will depend

on the work being undertaken, but we recommend that you back up on at least a nightly basis.

You may also want to use ADSM to back up some of the files included in the mksysb to make recovery faster in the event of damage or accidental deletion. We recommend that you back up the root file system and the /var file system on a nightly basis with ADSM to facilitate speedy recovery of any individual files. We do not recommend that the root file system be restored as a whole onto a running system.

By building a tailored include list for your ADSM backups, you should be able to recover from all but a complete system loss in a very short time. By including a mksysb backup whenever the system is changed or new software is installed, this recoverability should extend to any system damage.

Note:

By storing the system configuration information in DRM and using DRM to manage offsite storage of your ADSM and mksysb backups, recovery protection extends to the loss of the **whole site**. For more information about using DRM, see *ADSM for AIX: Advanced Topics* (SG24-4601-00).

13.3 Postdisaster Recovery

In this section we describe how to recover from a disaster to the AIX Version 3.2.5 ADSM client environment using the information we saved before disaster (described in 13.2, “Predisaster Preparation” on page 221) and the bootable tape we created (described in 13.2.3, “Creating the Bootable Mksysb Tape” on page 225).

To simulate the disaster, we removed all volume groups from the disks and ran the `rm -r *` command in the root directory to recursively remove all files from the system.

Using the information we had saved before the disaster, the mksysb tape we created, and the ADSM backups, we were able to completely recover the client machine as described below.

13.3.1 Rebuild Hardware Environment

Retrieve information about the AIX Version 3.2.5 machine to help re-create the hardware environment of the destroyed ADSM client, because the new replacement machine should have a similar configuration.

If you used DRM as the repository for information about the AIX Version 3.2.5 machine, retrieve it by issuing the appropriate queries to the ADSM server. For examples of these queries, see 1.3.6, “Disaster Recovery Manager” on page 18.

13.3.2 Boot the Recovery System

Once the hardware problems on the machine have been resolved or a new machine has been prepared, attach and power on the tape drive, place the mksysb tape in the tape drive, turn the system key to the **Service** position, and power on the machine.

When the menu appears, select `Restore a system from a mksysb image`. You then have the option to set the disks you want to install to. It is important that you select enough total disk space to accommodate your original system image (see the df output). After you have selected the settings, select the option to continue and restore the system.

The system will reboot, and you will be prompted to enter your user name and password. Login as root, and with the information collected before the disaster, use SMIT to re-create all extra LVs, VGs, and file systems. Use the menus under the `smit lvm` fast path shown below.

```
                              Logical Volume Manager

Move cursor to desired item and press Enter.

  Volume Groups
  Logical Volumes
  Physical Volumes

F1=Help             F2=Refresh          F3=Cancel           F8=Image
F9=Shell            F10=Exit            Enter=Do
```

You can now use ADSM to restore the file system data. Use this command:

```
dmsc restore -fromdate=XX/XX/XXXX -todate=LATEST subdir=yes \
/source-file-system /target-file-system
```

where XX/XX/XXXX is the date on which the mksysb was taken.

You can use the above procedure to restore all user data files on the system to their latest levels.

If configuration changes have taken place since the last mksysb, you can also selectively restore the `smit.script` file and run it, using:

```
cat /smit.script | ksh
```

Note:

Check through the smit.script file before executing to ensure that there are no commands that may cause problems on your new system. Watch for volume group operations and other commands that access the physical volumes.

13.3.2.1 Restoring a Volume

The easiest way to recover from the loss of a single PV in a VG is to replace the disk, re-create the VG, and then restore the data back to the newly created VG.

13.3.2.2 Restoring a File

You can restore a single file as usual from the ADSM backup. If, however, you have to restore a single file from the mksysb tape, use this procedure:

- Place the tape in the tape drive and check that the tape drive is available for use: `lsdev -Cc tape`
- Use `tctl -f /dev/rmtX.1 rewind` to rewind the tape.
- Use `tctl -f /dev/rmtX.1 fsf 3` to skip to the beginning of the fourth tape image, the tar data archive.
- Use `tar -xvf /dev/rmtX.1 ./` *path_name*/*file_name* to restore the file.

This procedure restores a single file to its original location. To restore files to new locations, specify a target path and file name after the source path and file name.

Note:

Remember the *"."* in front of the source path and file name. The files will be stored in *relative* format on the tape.

13.3.2.3 Verify the Postdisaster Restoration

At this point, you would use any statistics you saved with your ADSM backups and bootable image to verify that they are comparable to those you receive after your recovery is complete.

13.3.2.4 Other Methods

Other methods of system backup are available, such as IBM's Sysback/6000. This software enables direct disk-image backups over the network, thus conserving paging space definitions, ACLs, and logical volume placement information. Sysback is not a directly supported software product, however, and we therefore did not use it for our project. Much of the function of Sysback has been incorporated into the base AIX operating system at AIX Version 4.1 and above.

For more information about Sysback/6000 and AIX Version 4.1, contact your marketing or sales representative.

Chapter 14. AIX Version 4.1 Recovery

In this chapter we review the following techniques to recover an AIX Version 4.1 client environment that uses TCP/IP to communicate with its ADSM server:

- Mksysb restore
- Network Install Manager restore

We discuss the kind of information that should be backed up in preparation for a disaster, how to prepare for the MKSYSB or Network Install Manager restore, and how to use these techniques in conjunction with the previously saved information to recover an AIX Version 4.1 environment after a disaster.

14.1 Product Overview

AIX is a multiuser, multitasking operating system based on the UNIX model. With the arrival of Version 4.1, the variety of RS/6000 platforms on which AIX can be used increased to include SMP machines and the PCI-based RSPC models. Many new usability and performance features have been added as well as a new GUI known as the Common Desktop Environment (CDE). AIX Version 4.1 still uses the concept of logical volumes, file systems, and volume groups, as defined in 13.1.1, “Storage” on page 219, but the concept has been extended to allow larger file sizes, larger file systems, and logical volume striping. Striping allows the data to be spread across the disks so that their transfer capacity can be used in parallel, thus improving I/O performance.

14.1.1 Backup

A number of enhancements have been made to the mksysb utility in AIX version 4.1. Mksysb now allows a logical partition map to be stored with the backup that preserves logical volume placement. AIX Version 4.1 mksysb now automatically restores paging space definitions and ACLs. System backup in general has also been enhanced and now allows external volume groups to be backed up, similarly to `mksysb` through the `mkvgdata` and `savevg` commands.

14.1.2 Network Install Manager

Network Install Manager (NIM) is a new utility in AIX Version 4.1 that enables machines to be installed and maintained across a network from a central server. NIM supports clients on either *diskless, dataless,* or *stand-alone* mode and can operate over Ethernet, token-ring, and FDDI

networks. By defining a number of resources at the server to each client machine, the client machines can boot, install, and run using the server code. All operations can be configured to be initialized from either the client or the server console. For more information about NIM see the *AIX Version 4.1 Network Installation Management Guide and Reference*, SC23-2627-02.

Note:

The AIX Version 4.1 install process no longer loads all supported device drivers onto the hard disk. Therefefore a mksysb image produced at AIX Version 4.1 will have the device drivers for the source machine only and therefore cannot be restored to anything but an identical machine. We have looked at this issue and discuss it in 14.2.3, “Creating a Mksysb Image” on page 238.

14.2 Predisaster Preparation

The disaster we are preparing for is the total and catastrophic loss of the ADSM client, where provision has to be made to restore everything from the bare metal up. If our disaster recovery preparations can cover this worst case scenario we can assume that they will also be able to handle recovery from lesser disasters.

In this section we discuss the information to collect and save before a disaster to enable a bare metal restore.

14.2.1 ADSM Backups

For this test we divided all data on the system into *user data* and *system data*. We used either mksysb or NIM to back up and restore the system data and managed the user data with ADSM. We defined system data as the file systems necessary to the base operating system (BOS); this is usually the /,/usr, /var, and /tmp file systems. We defined user data as anything that is not included in system data.

For the purpose of this test we used the default include/exclude list for an ADSM UNIX client and specified that only the `/smit.script` file be additionally backed up by ADSM, to minimize the frequency at which we had to make new system backups.

We also set the copy group to use shared static option to avoid fuzzy backups.

If your system uses Hierarchical Storage Management (HSM), see *Using ADSM Hierarchical Storage Management*, SG24-4605, for more information.

For more information about using and configuring the ADSM client on AIX, see *ADSTAR Distributed Storage Manager Using the UNIX Backup-Archive Clients Version 2*, SH26-4052-00, and *Getting Started with ADSM AIX Clients*, GG24-4243-00.

14.2.2 Operating Environment of the ADSM Client

In preparation for disaster recovery we recommend that you collect and save offsite the information listed below in addition to the ADSM backup data. Depending on your installation, you could save this information by using the DRM feature, or you could save it on hardcopy stored offsite. The way in which you save the information is not as important as ensuring that it is saved **somewhere** where it can be easily retrieved along with the client recovery media when a disaster occurs.

- **Hardware configuration**

  Use the `uname -m` command to collect information about the machine type. This will return a 13-digit code of the form xxyyyyyymmss, where xx is always zero and indicates the system, yyyyyy indicates a unique identification number for the whole system, mm indicates a two-character code for the machine type, and ss indicates the submodel number and should always be zero. To match the machine type number against the list in the manual page for the uname command, issue `man uname`. Information about the installed hardware in the machine is included in output from the `lscfg -v` command. The output lists all adapters in the machine and specific information about their model, make, and microcode level where appropriate.

- **Logical storage information**

  Information regarding the storage setup of the client machine is vital to system recovery. The size of all disks in each VG, the number of LVs in each VG, and the size of each LV should be stored before the disaster in either hardcopy or within DRM.

  To list the physical disks per VG, issue this command:

  `lsvg -p` *vgname*

  To list the LVs per VG, issue this command:

  `lsvg -o | lsvg -i -l`

  To list details about each LV, issue this command:

  `lslv` *lvname*

Note:

If your system uses logical volume mirroring, you can gather information about the number of copies and their physical placement, using:

`lslv -m` *lvname*

- **Communications details**

  The information necessary to document your communications setup will depend on which protocol you are using. For TCP/IP note such items as the internet address, host name, default gateway, and netmask and for more detailed information a copy of the output from:

  `lsattr -l` *adapter name* `-E`

  For example, this command will produce the output shown below:

  `lsattr -l tr0 -E`

```
mtu       1492           Maximum IP Packet Size for This Device     True
mtu_4     1492           Maximum IP Packet Size for This Device     True
mtu_16    1492           Maximum IP Packet Size for This Device     True
remmtu    576            Maximum IP Packet Size for REMOTE Networks True
netadddr  129.33.160.145 Internet Address                           True
state     up             Current Interface Status                   True
arp       on             Address Resolution Protocol (ARP)          True
allcast   on             Confine Broadcast to Local Token-Ring      True
hwloop    off            Enable Hardware Loopback Mode              True
netmask   255.255.255.0  Subnet Mask                                True
security  none           Security Level                             True
authority                Authorized Users                           True
broadcast                Broadcast Address                          True
```

Note:

You can collect all of the above information and store it in a single file. Construct a shell script that will collect the information about each item and then add it to a specified file either for inclusion into the DRM or for back up and restore after a disaster.

For example, this shell script gathers information about the details and physical placement of each LV on the system:

```
for i in lsvg do
        for j in lsvg -l $i | cut -d" " -f1
        do
            echo "$i/$j:\n"
            echo "Details:"
            lslv $j 2> /dev/null
            echo "\nLocations:"
            lslv -l $j 2> /dev/null
            echo "\n"
            echo "═══════════════════════════════════════════════════"
        done done
```

If you make this script executable and run it with:

`./script >> /tmp/sys_info` file.

it will append (>>) the information to the end of the /tmp/sys_info file.

To enter the name and location of this file into the recovery information entry for that machine's definition in DRM, issue this command:

```
adsm> insert machine machinename sequencenumber \
recoveryinstructions="Machine Configuration Stored in /tmp/sys_info"
```

Optional: Statistics for Postdisaster Recovery Verification

You may want to collect and save information that you can use after a disaster once the restore process is complete to validate that all information has indeed been restored correctly. Each installation will have its own ideas about the best way to verify that the recovery is complete. Some possible sources of information for this type of verification are:

- Information about installed software (`lslpp -Al`)
- Size of data files (`ls -al`)

14.2.3 Creating a Mksysb Image

In this section we describe how to create the mksysb image for use as either a stand-alone tape recovery or an NIM recovery over the network.

14.2.3.1 Assumptions

These instructions should apply to any AIX Version 4.1.X system using ADSM.

The instructions apply to the following products:

- **AIX Version 4.1.X**
- **ADSM/AIX Version 1, Release 2 client code**
- **ADSM/AIX Version 2, Release 1 client code**
- **Any ADSM server.**

A complete ADSM backup as described in 14.2, “Predisaster Preparation” on page 234 should be available at the ADSM server, and the restore should be done to a hardware configuration similar to that of the original ADSM backup/archive client machine. For more information about restoring a mksysb backup to a dissimilar machine, see 14.3.5, “Other Topics” on page 257.

14.2.3.2 Configuration Used to Test This Technique

We tested this technique, using the following configuration:

- RS/6000 7013-320H with 128 MB RAM
- IBM High-Performance Token-Ring Adapter (093F1277)
- Four 1 GB and two 400 MB SCSI-attached disk drives
- Internal IBM 2.3 GB 8 mm tape drive
- Internal IBM SCSI quad speed CD-ROM

- AIX Version 4.1.4
- ADSM/AIX Version 2, Release 1, Level 3 client code
- ADSM/AIX Version 2, Release 1, Level 9 server code

To use the mksysb tape method, you will need:

- Internal or external direct-attached tape drive
- A copy of the AIX install media
- One blank data grade tape

To use the NIM method you will need:

- Another RS/6000 machine running a higher or equal level of AIX 4.1, connected to the client through TCP/IP
- A copy of your AIX install media
- Internal or external direct-attached tape drive or CD-ROM
- One blank AIX-formatted diskette

Note:

NIM setup assumes the following:

- NFS and TCP/IP are installed and configured.
- All networks to be part of the NIM environment are configured.
- Gateways are initialized.
- Name resolution is configured so that all machines that will be part of the NIM environment have resolvable host names.

14.2.3.3 Separating User Data and System Data

The method of separating user data and system data enabled us to limit the amount of data, and thus the time taken for the mksysb, while providing users with the advantages of conventional ADSM backup and restore.

We also used the root `smit.script` file as a log for any changes made to the system configuration between mksysb backups. If this file is cleared after each mksysb backup and reserved for any systemwide changes made between mksysbs, backing up this file with ADSM on a nightly basis meant that we had a way of recovering the system to last night's configuration without taking a mksysb every night. This file can be restored from ADSM after a mksysb restore and executed to update the system config to the latest level.

If you intend to use NIM to restore your system, go to 14.2.3.4, “Preparing the NIM Server” on page 243.

Preparing the System for Mksysb: Decide on a suitable time for the mksysb image to be taken of the system. The time is best when there is as little user activity as possible. Although user activity should not be able to compromise the integrity of the mksysb, system performance will be hit severely during the backup.

To ensure that the tape drive you intend to use is defined to the system and available for use, issue this command:

```
lsdev -Cc tape
```

This should produce output similar to the following:

```
rmt0 Available 00-08-00-3,0 2.3 GB 8mm Tape Drive
```

Use the df command to check which file systems are mounted an unmount any non-system-data file systems, using the unmount command. The only file systems that should be included in the df output should be these:

```
 Filesystem    512-blocks      Free %Used    Iused %Iused Mounted on
/dev/hd4           16384      5376   68%     1445     36% /
/dev/hd2         1507328    371008   76%    17625     10% /usr
/dev/hd9var        24576     22272   10%      126      4% /var
/dev/hd3           24576     21984   11%       64      2% /tmp
```

The system is now ready to be backed up.

Backing Up the System to Tape: First build the image.data file, which stores information about the sizes of the file systems for re-creation at restore time. It is vital this be done before a mksysb is taken of your system. Use the mkszfile command to create a mksysb:

```
mkszfile&&mksysb /dev/rmtX.1
```

where && indicates that the second command, the mksysb, should be started only if the mkszfile command completes successfully.

Note:

The mkszfile may fail if fewer than 500 blocks are free in any of the file systems. Check this by looking at the output of the df command and checking the Free column for each file system.

The X refers to the number of the tape drive you want to use and the .1 means that the tape should not be rewound after each end of file marker. If the .1 extension is not added, each image on the mksysb will overwrite the subsequent image and the tape will no longer boot.

You should do a test boot from your mksysb to ensure you have captured all required files. You can also check the data with:

```
tctl -f /dev/rmt0.1 rewind
tctl -f /dev/rmt0.1 fsf 3
restore -Tvf /dev/rmt0.1
```

Note:

If the machine you are using is a PCI-based machine, you cannot boot from the mksysb tape. This is a limitation of the bus architecture and may not be solved in software. To restore a mksysb on a PCI-based machine, you must first boot from the install CD and then select the option to restore from a mksysb on tape.

The mksysb command can also be run through SMIT with a fastpath of either smit startup or smit mksysb. This will automatically run the mkszfile command before backing up and will provide the .1 onto the tape drive name.

Note:

Performing a mksysb through SMIT runs the mkszfile command automatically, checks for space requirements, checks the device extension for tape drives, and checks to see whether the tape will be bootable.

Where possible, we would strongly advise initiating a mksysb through SMIT. This also has the advantage that all command output is logged in the smit.log file for future reference.

The smit mksysb screen is shown below.

```
                              Back Up the System

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

(TOP)                                                  (Entry Fields)
    WARNING:  Execution of the mksysb command will
              result in the loss of all material
              previously stored on the selected
              output medium. This command backs
              up only rootvg volume group.

* Backup DEVICE or FILE                               ( )              +/
  Create MAP files?                                    no              +
  EXCLUDE files?                                       no              +
  Make BOOTABLE backup?                                yes             +
     (Applies only to tape)
  EXPAND /tmp if needed?                               no               +
     (Applies only to bootable tape)
  Number of BLOCKS to write in a single output         ( )              #
     (Leave blank to use a system default)


F1=Help             F2=Refresh          F3=Cancel           F4=List
F5=Reset            F6=Command          F7=Edit             F8=Image
F9=Shell            F10=Exit            Enter=Do
```

The Create MAP files option, if selected, creates a map of the logical to physical partitions for each logical volume being backed up. This map will then be used to restore logical volume placement on restore. The Exclude files option can be used to point to a file that contains a list of files that should not be backed up with mksysb. We recommend leaving the Number of BLOCKS to write a single output at the system default.

Now, remount the file systems that you unmounted before the backup and zero the smit.script file on the root directory with the following command:

```
>/smit.script
```

If you have changed the default home directory of the root user, this smit.script file will be stored in that directory instead of the root directory.

Note:

Use the smit.script file to automate this task as well. Clear the file, use SMIT as root to unmount any file systems, and then mksysb the system. On completion use SMIT again to remount the file systems.

Rename the resulting smit.script file and use it with the AIX cron utility to automate the backup procedure.

If you are following the tape method, go to page 252, Backing Up User Data with ADSM.

14.2.3.4 Preparing the NIM Server

Note:

The information in this section is taken from the *AIX Version 4.1 Network Install Management Guide and Reference*, SC23-2627-02. We recommend that you obtain a copy of that document. It covers the issues addressed below in greater depth and may be used to deal with any problems you may encounter during the NIM setup and any differences between the configuration mentioned here and your own.

Before you begin setting up any NIM environment it is always a good idea to make a drawing of your network configuration and decide which machine is to be the NIM master. The NIM master must adhere to certain criteria:

- It must be running AIX Version 4.1 or at least the same level as the clients in its environment.
- It must have a stand-alone configuration and be able to communicate with all machines in its environment.
- It should ideally have a large disk resource to store the resources for the machines in its environment.
- It should be in a convenient location for the person administering the NIM environment.

Figure 40 on page 244 shows a sample NIM environment.

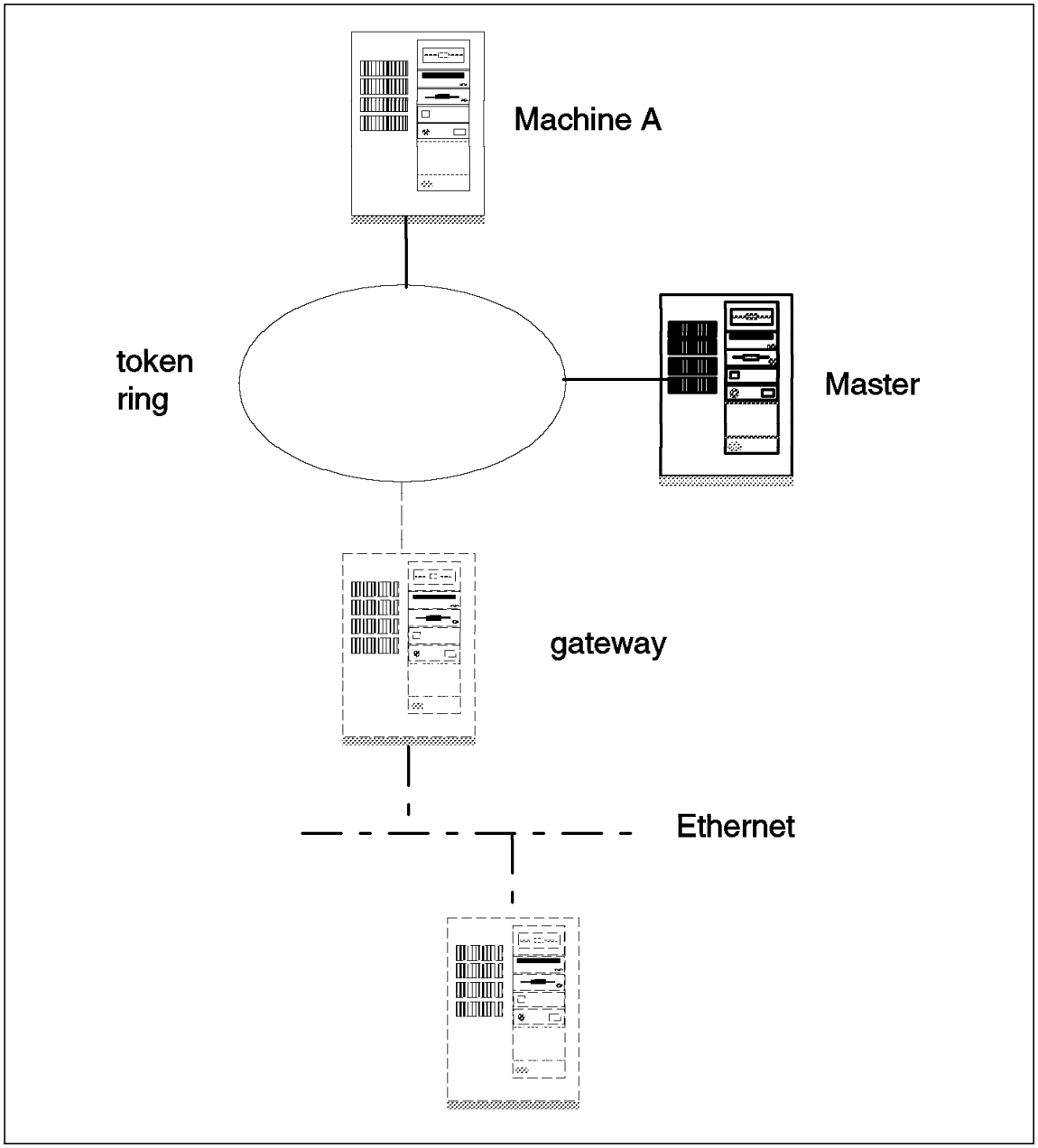


Figure 40. Sample NIM Environment Before Configuration

We will install Machine A in Figure 40 and discuss the additional configuration for installing Machine B.

Once you have decided on the machine you want to use as your NIM master, make sure that the bos.sysmgt.nim.master fileset is installed. Place the install media in the appropriate drive and run:

```
installp -a -g -X -d device_name bos.sysmgt.nim.master
```

where *device_name* is the name of the device containing your install media, for example, /dev/cd0.

Create the file systems necessary for NIM operation. These may initially be created as a small size and then extended later. Use:

```
crfs -v jfs -g rootvg -a size=8192 -m export -A yes

mount /export

mkdir /export/nim

mkdir /export/nim/scripts
```

To activate the NIM master, you must supply:

- A name for the primary network object, Network1, for example.
- Two consecutive port numbers for NIM operations. The default is ports 1058 and 1059. To avoid conflicts, check the reserved ports in the /etc/services file.
- The name of the primary network interface, in our case, tr0. For a list use:

  ```
  lsdev -C -c if -S available
  ```

- If the machine connects through a token ring, you also have to know the ring speed (4Mbps or 16 Mbps) and the cable type (bnc or dix).

Now activate the NIM master, using the SMIT fast path smit nimconfig or from the command line, using a command similar to:

```
nimconfig -a netname=Network1 -a master_port=1058 -a pif_name=tr0 -a  \
ring_speed=16
```

This command will configure an NIM master on Network1, which is a 16Mbps token-ring network. It will use port number 1058 for primary communications.

To check the status of the NIM master at this stage, run:

```
lsnim -l master
```

which should produce output similar to this:

```
master:
   class       = machines
   type        = master
   Cstate      = ready for a NIM operation
   reserved    = yes
   platform    = rs6k
   serves      = boot
   serves      = nim_script
   comments    = machine which controls the NIM environment
   Mstate      = currently running
   prev_state  =
   if1         = network1 KINDU.ALMADEN.IBM.COM 10005AB1B290
   master_port = 1058
   ring_speed1 = 16
```

If your environment involves any other networks, you must now define those networks to the NIM master. To define the Ethernet network, Network2, use:

```
nim -o define -t ent -a net_addr=129.33.72.0 -a snm=255.255.255.0 \
Network2
```

At this point you can use the `lsnim -l Network2` command to check the state of this network:

```
Network2:
   class      = networks
   type       = ent
   net_addr   = 129.33.72.0
   snm        = 255.255.255.0
   missing    = route to the NIM master
   Nstate     = information is missing from this object's definition
   prev_state =
```

The Nstate shows that there is some information missing from the objects definition. We next need to define a route between the primary network Network1 and this new network Network2 .

To do this we may use the SMIT `smit nim_mkroute` fast path or this command:

```
nim -o change -a routing1='Network2 gw1_tok gw1_ent' Network1
```

where *gw1_tok* is the hostname of the token-ring interface on the gateway machine, and *gw1_ent* is the hostname of the Ethernet interface on the gateway machine. We now have a route from Network1 to Network2.

14.2.4 Preparing the NIM Client

The first thing that you must take note of when you attempt to introduce a machine as a client into an NIM environment is the adapter hardware address. Enter :

```
lscfg -l adapter_name -v
```

where *adapter_name* is the logical device name of the adapter the client will use to access NIM resources, for example: tok0, ent0 or fddi0. Find and write down the Network Address entry and note down the value. For example,

```
Network Address.............10005AC94537
```

The next step is to determine whether your machine is capable of issuing a network BOOTP request on startup. The method of determining this varies from machine to machine and is discussed in Chapter 4 “Hardware-Related Tasks,” of the *AIX Version 4.1 Network Installation Management Guide and Reference*, SC23-2627-022. For a microchannel machine, you have to determine whether it is BOOTP-enabled with:

```
/usr/sbin/bootinfo -q adapter_name
```

This will return a 1 if the machine is BOOTP enabled.

The machine we used for this test was not BOOTP enabled and thus we had to execute the BOOTP from diskette. Place an *IPL-ROM emulation diskette* in the diskette drive of the NIM master and enter:

```
bosboot -r /usr/lpp/bos.sysmgt/nim/methods/IPLROM.emulation -d /dev/fd0 \
-M both.
```

We are now ready to introduce our client machine into the NIM environment. To define MachineA on Network1 to the NIM master, on the master machine enter:

```
nim -o define -t standalone -a platform=rs6k -a if1='Network1 host_name
10005AC94537' -a ring_speed1=16 MachineA
```

Where *host_name* is the host name of the client machine. Define MachineB on the Ethernet network in the same way:

```
nim -o define -t standalone -a platform=rs6k -a if1='Network2 host_name
10005AB1B290' MachineB
```

You are now ready to define your resources for NIM installation (see Figure 41 on page 248).

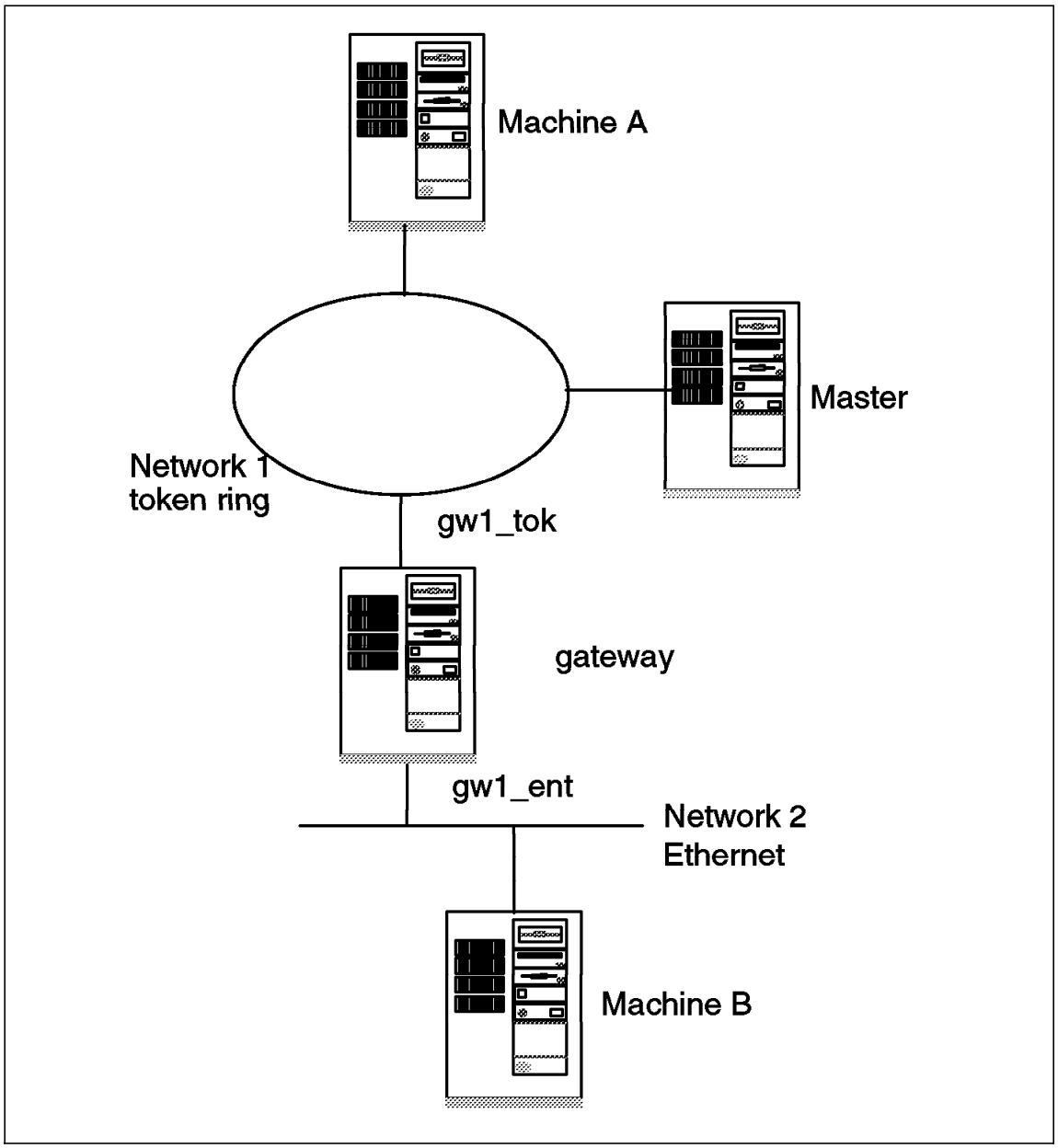


Figure 41. NIM Environment after Configuration

Before a base operating system install (bos_inst) operation can be performed on a stand-alone NIM client, the following resources must be created and allocated to the client:

- lpp_source with the simages attribute
- spot

For this method you will also allocate:

- bosinst_data
- mksysb

The lpp_source object contains software packages that are used during software installation. To be given the support-images simages attribute, this must contain:

- bos
- bos.rte.up
- bps.rte.mp
- bos.diag
- bos.net
- bos.sysmgt
- devices.all
- bos.terminfo

1. To create an **lpp_source**, place the installation tape or CD-ROM in the drive of the NIM master and enter:

   ```
   crfs -v jfs -g rootvg -a size=614400 -m /lpp_images -A yes

   mount /lpp_images

   nim -o define -t lpp_source -a location=/lpp_images -a server=master
   -a source=/dev/cd0 images
   ```

   This procedure may take up to one hour to complete.

2. To create the spot resource, first define the file system for the network boot images and mount it as /tftpboot:

   ```
   crfs -v jfs -g rootvg -a size=57344 -m /tftpboot -A yes

   mount /tftpboot
   ```

   Define the spot as spot1:

   ```
   nim -o define -t spot -a location=/usr -a server=master -a
   source=images spot1
   ```

This procedure may take up to one hour to complete.

You are now ready to take a mksysb of the client system. You can either:

- Take a bootable mksysb of the client system to tape, as described on page 226, Preparing the System for Mksysb, and "Backing Up the System to Tape" on page 240.

  Then, with the tape in the NIM master's tape drive, issue:

  ```
  mkdir /export/nim/mksysb

  crfs -v jfs -g rootvg -a size=XXXX -m /export/nim/mksysb -A yes

  mount /export/nim/mksysb

  cd /export/nim/mksysb

  tctl -f /dev/rmt0.1 rewind

  tctl -f /dev/rmt0.1 fsf 3

  dd if=/dev/rmt0.1 of=machine_name.mksysb bs=62b conv=sync
  ```

  where XXXX is a size (in 512-byte blocks) large enough to hold the mksysb image. You can estimate this size by looking at the `df` output on the running client system.

  This will copy the mksysb image from the tape onto the disk in the `/export/nim/mksysb` directory.

  OR

- Prepare the client system as shown on page 226, Preparing the System for Mksysb, and then NFS mount the /export/nim/mksysb file system onto the client and use `smit mksysb` with the following settings:

```
                              Back Up the System

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

(TOP)                                                  (Entry Fields)
    WARNING:  Execution of the mksysb command will
              result in the loss of all material
              previously stored on the selected
              output medium. This command backs
              up only rootvg VG.

* Backup DEVICE or FILE        (/export/nim/mksysb/machine_name.mksysb)
  Create MAP files?                                    yes
  EXCLUDE files?                                       no
  Make BOOTABLE backup?                                no
     (Applies only to tape)
  EXPAND /tmp if needed?                               no
     (Applies only to bootable tape)
  Number of BLOCKS to write in a single output         ()
     (Leave blank to use a system default)

F1=Help             F2=Refresh          F3=Cancel           F4=List
F5=Reset            F6=Command          F7=Edit             F8=Image
F9=Shell            F10=Exit            Enter=Do
```

This will then take a mksysb to the /export/nim/mksysb directory as a machine_name.mksysb file.

Once you have the mksysb on the NIM master, you can define it as a resource, **mksysb1**, with:

```
nim -o define -t mksysb -a server=master -a
location=/export/nim/mksysb/machine_name.mksysb mksysb1
```

If you want the restore to proceed without supervision or user input, you also have to define a bosinst_data resource to provide the NIM with the answers to some installation questions. Enter:

```
mkdir /export/nim/files

cp /var/adm/ras/bosinst.data /export/nim/files/bosinst.mydata

nim -o define -t bosinst_data -a server=master -a \
location=/export/nim/files/bosinst.mydata inst_answers
```

This will produce a resource named inst_answers, which you must edit using a text editor. Here is a sample file:

```
control_flow:
    CONSOLE =
    INSTALL_METHOD = overwrite
    PROMPT = yes
    EXISTING_SYSTEM_OVERWRITE = yes
    INSTALL_X_IF_ADAPTER = yes
    RUN_STARTUP = yes
    RM_INST_ROOTS = no
    ERROR_EXIT =
    CUSTOMIZATION_FILE =
    TCB = no
    INSTALL_TYPE = full
    BUNDLES =

target_disk_data:
    LOCATION = 00-00-0S-0,0
    SIZE_MB = 1920
    HDISKNAME = hdisk0
```

Headers in the file itself explain the meaning of each entry. The important fields are:

- CONSOLE - set to point to your console.
- INSTALL_METHOD - set to overwrite.
- PROMPT - set to no
- The **target_disk_data** stanzas have to be set, one for each disk you want in rootvg. Enter the location OR the size OR the disk name, for each.

Once you have defined all of these resources you are prepared for bare metal restore. You can define more resources and use them to customize the procedure. For more information see 14.3.5, “Other Topics” on page 257.

Backing Up User Data with ADSM

You must now back up any user data on the system that was not in the file systems backed up by the mksysb. Include the /home file system, any file systems in the rootvg that you created manually, and all file systems in external VGs. The regularity with which you back up this data will depend on the work being undertaken, but we recommend that you back up on at least a nightly basis.

You may also want to use ADSM to back up some of the files included in the mksysb to make recovery faster in the event of damage or accidental deletion. We recommend that you back up the root file system and the /var file system on a nightly basis with ADSM to facilitate speedy recovery of any

individual files. We do not recommend that the root file system be restored as a whole onto a running system.

By building a tailored include list for your ADSM backups, you should be able to recover from all but a complete system loss in a very short time. By including a mksysb backup whenever the system is changed or new software is installed, this recoverability should extend to any system damage.

Note:

By storing the system configuration information in DRM and using DRM to manage offsite storage of your ADSM and mksysb backups, recovery protection extends to the loss of the **whole site**. For more information about using DRM, see *ADSM for AIX: Advanced Topics* (SG24-4601-00).

14.3 Postdisaster Recovery

In this section we describe how to recover from a disaster to the AIX Version 3.2.5 ADSM client environment using the information we saved before disaster (described in 13.2, “Predisaster Preparation” on page 221) and the bootable tape we created (described in 13.2.3, “Creating the Bootable Mksysb Tape” on page 225).

To simulate the disaster, we removed all volume groups from the disks and ran the `rm -r *` command in the root directory to recursively remove all files from the system.

Using the information we had saved before the disaster, the mksysb tape we created, and the ADSM backups, we were able to completely recover the client machine as described below.

14.3.1 Rebuild Hardware Environment

Retrieve information about the AIX Version 4.1 machine to help re-create the hardware environment of the destroyed ADSM client, because the new replacement machine should have a similar configuration.

If you used DRM as the repository for information about the AIX Version 3.2.5 machine, retrieve it by issuing the appropriate queries to the ADSM server. For examples of these queries, see 1.3.6, “Disaster Recovery Manager” on page 18.

If you backed up your system with NIM go to 14.3.3, “Complete System Recovery Using NIM” on page 254.

14.3.2 Complete System Recovery Using Mksysb Tape

Once the hardware problems on the machine have been resolved or a new machine has been prepared, attach and power on the tape drive, place the mksysb tape in the tape drive, turn the system key to the Service position, and power on the machine.

Then, when the Welcome to Base Operating System Installation and Maintenance menu appears, select 3 Start Maintenance Mode for System Recovery.

Then select 4 Install from a System Backup

Follow the instructions on the screen to select the language and disks you want to install to. It is important that you select enough total disk space to accommodate your original system image (see the df output). After you have selected the settings, select the option to continue and restore the system.

Note:

If you are using an RSPC model RS/6000, you will have to boot from the install CD-ROM and select the option to install from a system image backup.

The system will reboot and you will be prompted to enter your user name and password.

You are now ready to restore the user data that was stored in the ADSM backup. See 14.3.4, “User Data Recovery with ADSM” on page 256.

Note:

The tape-based mksysb method may be made to restore automatically, similar to the NIM method, with the bosinst.data file. See the *AIX Version 4.1 Installation Guide*. If you automate the restore, be careful that you do not try and use the tape to boot into maintenance mode as the restore will begin automatically.

14.3.3 Complete System Recovery Using NIM

Once you have repaired the hardware fault on the machine, you are ready to begin the restore of the software. During this stage let us assume you are using the IPL-ROM emulation media you created in 14.2.4, “Preparing the NIM Client” on page 247.

On the master you must prepare the resources for the client machine to be installed. The easiest way to do this is with the SMIT `smit nim_alloc` fast path. This will take you to a screen where you can select the client system and then select from a list, using the F7 key, the resources you want to allocate to it. Select the `lpp_source`, `spot1`, `mksysb`, and the `bosinst.data` resources. NIM automatically assigns a `nim_script` and `boot` resource for you.

To initiate the restore from the master:

1. Use the SMIT `smit nim_mak_op` fast path.
2. Select the machine name for the machine to be restored.
3. Select `bos_inst` from the list of operations.
4. Select `mksysb` to be the source of the BOS run-time files.
5. Press Enter to initialize the operation.

You will get an an error saying that the client machine cannot be rebooted because it is not up and running at this stage. You have to manually initiate a network boot.

To initiate a BOOTP request, using IPL-ROM emulation:

1. Insert the IPL-ROM emulation media into the appropriate drive on the client machine.
2. Turn the key to the `Service` position.
3. Power on the machine. The three-digit LED will display 260, 261, or 262 and then the `MAIN MENU` will appear. If the menu does not appear, wait a while and press Enter. A language selection may need to be made if this is the first time the system has booted using IPL-ROM emulation media.
4. Select the `Select BOOT (Startup) Device` option.
5. Select the network adapter from which the machine will boot. If you have multiple network adapters, type 88 and press the Enter key to view a list. If you are using a token-ring card, make sure that you select the entry with the correct ring-speed.
6. The next screen will be the SET OR CHANGE NETWORK ADDRESSES screen. The hardware address for the network adapter is displayed in the hardware address field. If the master and client are on the same network, you can leave the IP address fields blank, but if they are on different networks, you have to enter the IP addresses for the client, the master, and the gateway between them. We recommend that you always enter the IP addresses for client and master, just to be on the

safe side. Type 99 and press Enter to save the address information and return to the main screen.

7. To test the network connection, select Send Test Transmission (PING) from the menu.
8. Select Exit Main Menu and Start System (BOOT).
9. Follow the instructions on the screen to turn the key to the Normal position. Press Enter.

The BOOTP request should now be issued and followed by a Trivial File Transfer Protocol (TFTP) transfer of the network boot image.

If all resources have been defined correctly, the machine will now restore the mksysb and then reboot back to the login prompt. You are now ready to restore the ADSM backup of the system's user data.

14.3.4 User Data Recovery with ADSM

Login as root and, with the information collected before the disaster, use SMIT to re-create all extra logical volumes, volume groups, and file systems. Use the menus under the `smit lvm` fast path. The LVM main menu is shown below.

```
                          Logical Volume Manager

Move cursor to desired item and press Enter.

  Volume Groups
  Logical Volumes
  Physical Volumes

F1=Help             F2=Refresh          F3=Cancel           F8=Image
F9=Shell            F10=Exit            Enter=Do
```

You can now use ADSM to restore the file system data:

```
dmsc restore -fromdate=XX/XX/XXXX -todate=LATEST subdir=yes \
/source-file-system /target-file-system
```

where XX/XX/XXXX is the date on which the mksysb was taken.

Use this procedure to restore all user data files on the system to their latest levels.

If configuration changes have taken place since the last mksysb, you may now also selectively restore the `smit.script` file and run it using:

```
cat /smit.script | ksh
```

Note:

Check through the smit.script file before executing to ensure that there are no commands that may cause problems on your new system. Watch for volume group operations and other commands that access the physical volumes.

14.3.4.1 Restoring Files and File Systems

You can recover files and file systems from the ADSM backups as usual. Use the information saved previously to re-create any damaged file systems and then use ADSM to recover the missing files.

If the missing or damaged files are stored within the mksysb image, use the following procedure:

1. Place the tape in the drive and make sure that the tape drive is available for use, use `lsdev -Cc tape`.
2. Use `tctl -f /dev/rmtX.1 rewind` to rewind the tape.
3. Use `tctl -f /dev/rmtX.1 fsf 3` to skip to the beginning of the fourth tape image, the backup data archive.
4. Use `restore -xvf` */path_name/file_name* to restore the file to its original location.

You can also restore files to a new location by specifying a target path and/or file name.

14.3.5 Other Topics

You can use some advanced techniques to customize system recovery methods to your site and make them more versatile.

In this section we discuss some advanced techniques and explain how to use them to enhance the methods discussed so far.

14.3.5.1 Cloning Systems Using Mksysb

Here we include a copy of the IBM Technical Support fax (fax number 2540) that demonstrates how mksysb images from one machine can be restored onto another. Use this technique to restore mksysb images from a PCI-based machine to an MCA-based machine and a uniprocessor machine to a multiprocessor machine.

ABOUT THIS DOCUMENT

AIX 4.1 has been packaged so that only the devices that are needed are actually installed on the system. This has made the cloning process difficult. In 3.2, you were able to create a mksysb tape on one machine and install it on almost any other machine because most of the device drivers were in bos.obj.

In 4.1, the devices were separated from the base in separate filesets, devices.* (i.e. devices.scsi.disk). This, coupled with all the new hardware that has been released in the last 2 years (RSPC, SMP, graphics adapters, disks, etc) has made cloning machines almost impossible. Up to this point we have said that the only "supported" method of cloning was to install all the devices on a machine before you created a mksysb image. This is a waste of space because you don't need ALL the devices, but you don't know what devices you'll need until you're actually installing.

We've come up with a way to do this, but you still have to have a product media at the same level as your mksysb. This procedure is very important for not only cloning systems, but also for reproducing problems on different hardware.

TIPS FOR CLONING

Today, in 4.1, we have 2 kinds of platforms, rs6k and rspc. We also have 2 different kernels, up and mp. rs6k boot images are different from rspc boot images, and one will NOT boot the other. The rspc boot image has some specific boot information at the front of the image that the rs6k does not understand. To avoid this boot image mismatch problem, we advise using the product media, preferably a CD ROM, because it contains both boot images, so it will boot any system.

To find out what platform type your machine is, run the

```
   bootinfo -T

command.  To find out what kernel you system uses, use the

   bootinfo -z

command.

When using NIM to install your mksysb, you don't have to
worry about boot images or UP/MP because it will figure this
out for you.

There are two ways to clone a mksysb image in 4.1:

PHYSICAL MEDIA with CD-ROM product media, a mksysb tape and
          a customized diskette

NIM       with NIM resources and a mksysb image

 Both of these procedures have been tested with 4.1.4.0 media
 and install images.  This procedure has been tested with 413
 physical media, but hasn't been tested with 413 NIM.

PHYSICAL MEDIA PROCEDURE

 1.  Create a customized diskette.

        # mkdir /tmp/clone
        # cd /tmp/clone
        # echo data > signature
        # cp /var/adm/ras/bosinst.data .
        # vi bosinst.data

     Refer to the section "Customizing the BOS Install
     Program" in INFO for more details about creating a
     bosinst.data file.  You may want to customize it for
     your system to get a no-prompt install, in which case
     you will need to set more than is listed below (like
     CONSOLE and PROMPT).

     NOTE:  Make sure that the control_flow: stanza has this
     entry set (it's the most important part of the
     bosinst.data for this procedure):
```

```
This will run the tell bos install to run the cloner
script after it has restored the mksysb image.

Also, the target_disk_data stanza should be "zeroed" out
as shown below so that the bos install program will
install on the best fit disk(s).

Here is a sample bosinst.data file:

  control_flow:
      CONSOLE =
     INSTALL_METHOD = overwrite
     PROMPT = yes
     EXISTING_SYSTEM_OVERWRITE = yes
     INSTALL_X_IF_ADAPTER = yes
     RUN_STARTUP = yes
     RM_INST_ROOTS = no
     ERROR_EXIT =
     CUSTOMIZATION_FILE = cloner
     TCB = no
     INSTALL_TYPE =
     BUNDLES =

  target_disk_data:
     LOCATION =
     SIZE_MB =
     HDISKNAME =

  locale:
     BOSINST_LANG = C
     CULTURAL_CONVENTION = C
     MESSAGES = en_US
     KEYBOARD = en_US
```

2. Create the customization script

```
     # vi cloner
```

Sample Script:

```
  #!/usr/bin/ksh

  set -x
```

```
        RV=bootinfo -z
        if { "$RV" -eq 1 }
        then
        installp -abcgXd/../SPOT/usr/sys/inst.images bos.rte.mp
        ln -fs /usr/lib/boot/unix_mp /usr/lib/boot/unix
    fi

    if { "$RV" -eq 0 }
    then
        installp -abcgXd/../SPOT/usr/sys/inst.images bos.rte.up
        ln -fs /usr/lib/boot/unix_up /usr/lib/boot/unix
    fi

devinstall -b -d /../SPOT/usr/sys/inst.images -f /../tmp/device.pkgs

    cfgmgr -v -i /../SPOT/usr/sys/inst.images

    BLVDISK=lslv -l hd5 | grep hdisk | head -1 | cut -d' ' -f1
    ln -f /dev/r$BLVDISK /dev/ipldevice

    bosboot -a -d /dev/ipldevice

    rm -f /etc/firstboot

    sync
    sync
    sync

    exit 0
```

3. Backup the 3 files to a diskette:

```
# find . -print | backup -ivqf/dev/rfd0
```

4. Create a 414 mksysb tape from the system that you want to clone. It can be a UP system that you want to clone to an MP system, or a RISC box that you want to clone to an rspc. Any configuration should work.

5. Boot the target machine (the one you want to install on) with the AIX 4.1.4 CD ROM product media, and insert the diskette in the drive. Make sure the tape drive is turned on, but don't insert the tape yet as it might try to boot from the tape. Hit the PF1 key when the console

screen comes up, then hit enter when the language screen comes up (to get English). Then, when the:

```
   Welcome to Base Operating System
   Installation and Maintenance
```

screen comes up, choose #3,

```
   3 Start Maintenance Mode for System Recovery.
```

Then choose #4

```
   4 Install from a System Backup
```

Put the mksysb tape in the tape drive and close the door. Select the tape drive from that menu and hit enter. You will then see the system access the tape drive, then restore from the diskette drive. Then the confirmation screen will come up. Choose 1 or 2, hit enter, then hit enter again to confirm the install. If you're using 413, you will see the language menu come up after the tape is read and the diskette is restored. Just hit enter for the default English and you will get the confirmation install screen. Choose 1 or 2 and hit enter to start the install.

You can then turn the key (if there is a key) to normal at this time so the machine will reboot when the install is complete.

You should see the mksysb being restored, and then you should see installp called later when cfgmgr is called from the script to install any additional devices it detects.

WARNING: When installing a mksysb on a different platform type (e.g. an rs6k mksysb to an rs6ksmp, or an rs6k to an rspc) the first bosboot that bos install attempts will FAIL, and a message will be printed out to ask if you want to do maintenance or continue. You should continue at this point and the cloner script will run, although you will NOT see any output until the copyright screen at the end and the machine reboots.

NIM PROCEDURE

For complete documentation, see the NIM Guide in INFO - or order from PUBS - SC23-2671-01 Network Install Management Guide and Reference

Create the NIM environment by choosing and defining a master (see Chapter 3 - Setting up the Master and Network Objects). Each environment will be different, depending on your machine resources. Choosing which machine is the master, and which machines will be servers is a choice you must make based on your own environment.

In the following procedure, the master is the server for all resources. The CD ROM is the lpp_source. This will save space, but it also will keep the CD busy until all your client machines have been installed, something you may not want if you're using INFO from CD.

1. Create a 414 SPOT from your CD ROM See "Managing SPOT Resources" in INFO

   I created a separate 200 meg filesystem first called /414spot for non-/usr SPOT.

```
# mklv -y spotlv nimvg 50
# crfs -v jfs -d spotlv -m /414spot
# mount /414spot
# smitty nim_mkres
   spot            = Shared Product Object Tree

   * Resource Object Name           ·414spot‘
   * Resource Type                   spot
   * Server of Resource             ·master‘
   * Source of Install Images       ·/dev/cd0‘
   * Location of Resource           ·/414spot‘
```

2. Create an lpp_source with your CD-ROM (saves space) See "Managing lpp_source Resources" in INFO

```
# crfs -v cdrfs -d /dev/cd0 -m /CD -p ro
# mount /CD
# smitty nim_mkres
   lpp_source      = source device for optional
```

```
                                product images

          * Resource Object Name       ·414cd‘
          * Resource Type              lpp_source
          * Server of Resource         ·master‘
            Location of Resource       (/CD/usr/sys/inst.images)
```

3. Define the standalone client (target) machine See "Adding a Running Client to the NIM Environment" in INFO

   ```
   # smitty nim_mac
   Define a Machine Object
   ```

4. Create a mksysb image. You can make a mksysb image from smit on the machine you want to clone with "smitty mksysb". If the machine you're going to clone is not the NIM master, you can create a separate file system on the NIM master (I created /mksysb at 500 meg) and NFS mount it on the client, and backup to /mksysb/clone.image. This way you don't have to take up space on the client. If you have a mksysb tape that you want to use, you can get the image off the tape with the following procedure:

   ```
   tctl rewind
   tctl -f /dev/rmt0.1 fsf 3
   dd if=/dev/rmt0.1 of=/mksysb/clone.image
   ```

   Make sure your blocksize is set to the same blocksize the tape was made at.

5. Create and define a customized script. Create the script defined in the physical procedure (step 2). Put it in the mksysb directory, /mksysb/cloner.

   ```
   # smitty nim_mkres
   script          = an executable file which is
                     executed on a client

                  Define a Resource Object

   * Resource Object Name           ·cloner_script‘
   * Resource Type                   script
   * Server of Resource             ·master‘
   ```

```
        * Location of Resource           ·/mksysb/cloner‘
```

6. (Optional) Create and define the bosinst.data file.
   This is mostly used to enable ″no-prompt″ installs. See
   ″Customizing the BOS Install Program″ in INFO.

```
        # cp /var/adm/ras/bosinst.data /mksysb/bosinst.data
        # vi /mksysb/bosinst.data

        The following options should be set

        INSTALL_METHOD = overwrite
        EXISTING_SYSTEM_OVERWRITE = yes
```

   Also, target_disk_data stanza should be ″zeroed″ out
   like I have below so that the bos install program will
   install on the best fit disk(s).

```
              target_disk_data:
                LOCATION =
                SIZE_MB =
                HDISKNAME =

            # smitty nim_mkres
bosinst_data    = config file used during base system installation

     * Resource Object Name                ·clone_bosinst_data‘
     * Resource Type                       bosinst_data
     * Server of Resource                  ·master‘
     * Location of Resource                ·/mksysb/bosinst.data‘
```

7. Allocate 414cd, 414spot, (optional) clone_bosinst_data,
   cloner_script and clone_mksysb to the client.

```
        # nim -o allocate -a mksysb=clone_mksysb \
          -a bosinst_data=clone_bosinst_data \
          -a script=cloner_script \
          -a spot=414spot -a lpp_source=414cd (client)
```

8. Initiate the install on the client.

   See ″Initiating BOS Installation of Standalone Client″
   in INFO. If the target machine is already a nim client
   and running then initiate a push install

```
   # nim -o bos_inst -a source=mksysb (clientname)

If the target is not a NIM client but is running (ie,
installed at 3.2) then initiate a force push install

   # nim -o bos_inst -a source=mksysb -a force_push=yes

If the target is not running then initiate a pull
install

   # nim -o bos_inst -a source=mksysb -a no_client_boot=yes

Then go to the client machine and initiate the network
boot.  See "Initiating a BOOTP Request" in INFO for more
details on this.

WARNING:  YOU MUST BE AT THE NIM CLIENT FOR THIS CASE.
When installing a mksysb on a different platform type
(i.e. rs6k mksysb to rs6ksmp, or rs6k to rspc) the first
bosboot that bos install attempts will FAIL, and a
message will be printed out to ask if you want to do
maintenance or continue.  You should continue at this
point and the cloner script will run, although you will
NOT see any output until the copyright screen
```

Note: In the above squre brackets have had to be replaced with {}.

14.3.5.2 Postrestore Customization

Some sites, hay have many machines all with a similar base setup. In such cases it may be possible to make one mksysb image and then use the script resource to configure the differences from the base setup.

A script resource is executed during the customization phase of a a bos_inst operation. It can therefore be used to configure the TCP/IP network parameters and other tasks.

A script resource is an executable shell script that is run after the restore is complete. Here is an example:

```
#!/bin/ksh Script to set hostname, nameserver, DNS domain name
#          and routing table.
# Truncate the hostname
# if the hostname is fully qualified

chdev -l inet0 -a hostname =$(/usr/bin/hostname | cut -d. -f1)

# Set Nameserver and Domain Name

if {{ -f /etc/resolv.conf }}
then
    /usr/sbin/namerslv -E '/etc/resolv.conf.sv'
fi
/usr/sbin/namerslv -a -i '129.33.72.254'
/usr/sbin/namerslv -c 'almaden.ibm.com'

# Flush routing table and add default route

/etc/route -n -f
odmdelete -o CuAt -q "name=inet0 and attribute=route"
chdev -l inet0 -a route=net,,'0','129.33.72.254'
```

Note: The {} braces in the above represent square brackets.

Note:

To customize the restore even more, you can use the script resource to handle the re-creation of the VGs and LVs and even initiate the ADSM restore.

With a little bit of forward planning it should be possible to automate the entire procedure.

Appendix A. Alternative Methods to Create Base OS/2 Bootable Diskettes

In this appendix we describe two alternative methods for creating the base for the OS/2 bootable diskettes.

Booting an OS/2 system requires two diskettes. The first is identical to your installation disk 0 (and is henceforth referred to as disk 0). The second is similar to your installation disk 1, as it contains the command line OS/2 (CMD.EXE), your CONFIG.SYS, and any drivers that need to be loaded at boot time.

Attention

Bootable diskettes are sometimes very machine specific. For example, if you create the diskettes on a non-PS/2, they may not work on a PS/2. Either create the diskettes on a machine similar to the machine on which you want to use them or use another method that creates more generic diskettes.

A.1 CID Creation of OS/2 Base Diskettes

We did not use this method of creating the base OS/2 diskettes, but we include the instructions here for your reference.

If you have access to a server that provides CID installs, you can take advantage of its ability to create empty, bootable diskettes. Log on to the server, attach yourself to the CID directory, and execute the following:

```
DIRECTORY\SEdisk /S: <SOURCE PATH> /T: <TARGET DRIVE>
```

The source path and target drive are of course dependent on your setup. For example, when logged on to a particular CID system, executing either:

```
EXE\SEdisk /S:X:\IMG\OS2V30 /T:A:
```

or

```
EXE\21EXE\SEdisk /S:X:\IMG\OS2V21 /T:A:
```

creates two disks: a disk 0, and a half-empty, bootable disk 1. The first example creates OS/2 Warp (Version 3.0) diskettes; the second creates OS/2 Version 2.11 diskettes.

OS/2 WARP and OS/2 WARP Connect Users

The diskettes created by the OS/2 Warp Version of SEdisk contain some extra files that are not needed. To save space, you can delete the following files:

UNPACK.EXE
UNPACK2.EXE
XDFLOPPY.EXE

If you delete these files, be sure to remove XDFLOPPY from CONFIG.SYS to prevent extraneous errors at boot time.

You may want to ask your LAN administrator how the directories on your code server are set up. If you are the LAN administrator, see *Automated Installation for CID Enabled OS/2 V2.x*, GG24-3783, for instructions on installing and using SEdisk.

A.2 Create Utility Diskettes (OS/2 Warp and OS/2 Warp Connect)

We did not use this method for creating the base OS/2 diskettes, but we include the instructions here for your reference.

You can use the OS/2 Warp Create Utility Diskettes function to create the seed diskettes. Within your OS/2 System folder you should find an icon called System Setup. Within that folder you will find Create Utility diskettes, which guides you through the creation of three diskettes, which we call disks 0, disk 1, and disk 2. (Note that OS/2 Warp refers to them as disks 1, 2, and 3.)

Disks 0 and 1 are ready for Step 3 - you need not delete the files referred to in Step 2 as they are not created when this method is used.

Format disk 2.

Appendix B. Contents of Files Added to Bootable Diskettes

In this appendix, we outline the purpose and list the contents of each file that you have to create as part of setting up the bootable diskettes.

B.1 STARTUP.CMD

This startup file is kicked off by the command processor itself. It does the following:

1. Prints a banner
2. Calls FINDRAM.CMD to find the drive letter of the VDISK
3. Copies all command files and the editor to the VDISK
4. Chains to PART2.CMD to continue the initialization from the VDISK.

Create a STARTUP.CMD file and type in it the contents shown in Figure 42 (even spaces are important).

```
@ECHO OFF
ECHO ADSM BOOTABLE RECOVERY STARTED........
ECHO ******************************************
ECHO .
ECHO Searching for a VDISK
CALL FINDRAM.CMD
ECHO VDISK Found as drive %VDISK%:\
ECHO .
ECHO Copying Files to drive %VDISK%:\
COPY A:* %VDISK%:\ 1>NUL
COPY A:TEDIT.EXE %VDISK%:\ 1>NUL
ECHO .
PART2.CMD
```

Figure 42. STARTUP.CMD File

B.2 FINDRAM.CMD

FINDRAM.CMD is a small EXEC that locates the VDISK and saves its drive letter in an environment variable for later use. It works as follows:

1. Runs through all the drive letters
2. Creates a command file with ″@ECHO OFF″ in it
3. Appends to that command file the output of the VOL command

4. Runs that command file, which in turn:
5. Runs THE.CMD, which in turn:
6. Sets the VDISK environment variable to the drive letter of the VDISK

Create a file called FINDRAM.CMD and type in it the contents shown in Figure 43 (even spaces are important).

```
@ECHO OFF
FOR %%D IN (C D E F G H I J K L M N O P Q R S T U V W X Y Z) DO %%D: 2>NUL
ECHO @ECHO OFF>VOLDAT.CMD
VOL >>VOLDAT.CMD
CALL VOLDAT.CMD
```

Figure 43. FINDRAM.CMD File

B.3 THE.CMD

FINDRAM.CMD relies on an old batch file trick. Consider the output of the VOL command:

```
The volume label in drive D is DRIVE-D.
The Volume Serial Number is 6248:3630.
```

If you take the output, pipe it to a command file, and run it, the command processor looks at the first line and tries to run the **THE** command, passing the rest of the line as a command line parameter. We created a THE.CMD to catch this command line and parse it.

Create a file called THE.CMD and type in it the contents shown in Figure 44 as shown (even spaces are important).

```
SET VDISK=%5>NUL
```

Figure 44. THE.CMD File

The fifth parameter to be passed to this command file is simply the drive letter of the current drive. We assign this to an environment variable in memory.

The second line of the VOL command output that reads ″The Volume Serial Number is″ does not kick off THE.CMD and mess everything up because the command processor never gets to it. Because THE.CMD is ″chained,″ not ″called″ from VOLDAT.CMD, the process simply ends when THE.CMD ends.

However, the VOLDAT.CMD-THE.CMD process was ″called″ from FINDRAM.CMD, FINDRAM is returned to when the process ends. This may not be the simplest, most straightforward solution, but it works!

B.4 PART2.CMD

PART2 unpacks the ZipFile to the VDISK. If you are using UNZIP.EXE instead of the PKUNZIP2.EXE, change the SET UNZIPPER command to UNZIP (instead of PKUNZIP2). PART2.CMD:

1. Sets an environment variable to either PKUNZIP or UNZIP
2. Sets the system′s ETC and TMP variables for TCP/IP
3. Tells the user to insert the disk with the ZipFile and pauses
4. UnZips the archive from disk 2 to the VDISK
5. Asks the user to reinsert disk 1 and pauses
6. Chains to PART3.CMD

Create a file called PART2.CMD and type in it the contents shown in Figure 45 (even spaces are important). The only exception is this: If you choose the UNZIP utility instead of the PKUNZIP2 utility, change SET UNZIPPER=PKUNZIP2 to SET UNZIPPER=UNZIP.

```
@ECHO OFF
REM The following should be set to either PKUNZIP2 or UNZIP.
SET UNZIPPER=PKUNZIP2
SET ETC=%VDISK%:
SET TMP=%VDISK%:
ECHO Unpacking files to VDISK
ECHO Wait for all diskette activity to stop, (background processes...)
ECHO Remove diskette 1 from the drive, and insert diskette 2 and then
PAUSE
ECHO Working...
A:%UNZIPPER% -o A:ADSMPACK.ZIP
ECHO Done...
ECHO Please remove diskette 2 from the drive, and insert diskette 1 and then
PAUSE
PART3.CMD
```

Figure 45. PART2.CMD File

B.5 PART3.CMD

PART3 prompts you for information, configures ADSM and TCP/IP, and starts up TCP/IP for you. It begins by prompting you to edit SETUP.CMD; which is the EXEC that contains all of your settings (for example, ADSM node name). It consists of a series of SET VARIABLE=VALUE statements. Edit the values to correspond to the client being restored, and save the file. PART3 then runs the SETUP.CMD, which causes all these values to be loaded into memory and then uses them where necessary to configure ADSM and TCP/IP.

The process for PART3.CMD is as follows. It:

1. Runs the editor you copy to disk 1 to edit SETUP.CMD. (In the code shown in Figure 46 on page 275, the editor chosen is TEDIT, which is shipped with OS/2.).
2. Calls SETUP.CMD to load the variables into the environment
3. Sets your COMMMETHOD and NODENAME in DSM.OPT
4. Sets your TCPSERVER and TCPPORT in DSM.OPT
5. Sets your domain name and nameserver address in RESOLV for TCP/IP
6. Starts your TCP/IP interface using your address and subnet
7. Sets your TCP/IP default route
8. Informs the user that the setup is complete and drops to the command prompt.

Create a file called PART3.CMD and type in it the contents shown in Figure 46 on page 275 (even spaces are important). After you have created the file copy it onto disk 1.

```
TEDIT SETUP.CMD
CALL SETUP.CMD
ECHO .
ECHO Configuring ADSM
ECHO COMMMETHOD %COMMMETHOD% >>%VDISK%:\DSM.OPT
ECHO NODENAME %NODENAME%>>%VDISK%:\DSM.OPT
ECHO .
ECHO Configuring ADSM TCP/IP
ECHO TCPSERVERADDRESS %TCPServerAddress%>>%VDISK%:\DSM.OPT
ECHO TCPPORT %TCPPORT%>>%VDISK%:\DSM.OPT
ECHO .
ECHO Configuring ADSM NetBIOS
ECHO NETBIOSSERVERNAME %NETBIOSSERVERNAME%>>%VDISK%:\DSM.OPT
ECHO .
ECHO Configuring TCPIP
ECHO domain %domain%>>%VDISK%:\RESOLV
ECHO nameserver %nameserver%>>%VDISK%:\RESOLV
ECHO .
ECHO Starting TCP/IP
ROUTE -f
ARP -f
IFCONFIG lan0 %ADDR% netmask %SUBNET%
IFCONFIG lan0 UP
ROUTE add default %ROUTE% 1
ECHO .
ECHO Initialization Complete:  You may now start the ADSM restore...
```

Figure 46. PART3.CMD File

B.6 PART3A.CMD

PART3A allows you to change the contents of RESCUE1.INI, the parameter file for the CID Code Server and gives you the line command used to start it up.

Create a file called PART3A.CMD and type in it the contents shown in Figure 47 on page 276 (even spaces are important). After you have created the file, copy it onto disk 1.

```
@ECHO OFF
TEDIT RESCUE1.INI
ECHO Initialization Complete.
ECHO .
ECHO To Start the Code Server enter:
ECHO .
ECHO SERVICE /INI=RESCUE1
ECHO ********************
```

Figure 47. PART3A.CMD File

B.7 SETUP.CMD

You want the SETUP.CMD values that you start with to be as close as possible to the values you will use on the client that will be restored with the bootable diskettes. If, for example, each client has its own personal set of bootable diskettes, the SETUP.CMD could be tailored to be complete and accurate for that one client. If instead you have one set of diskettes for the restoration of many clients, you have to configure each client machine's TCP/IP address and ADSM node name at boot time. Any other values that all clients have in common could be stored in this file to save on editing SETUP.CMD at boot time.

Create a file called SETUP.CMD and type in it the contents shown in Figure 48 on page 277 (even spaces are important). After you have created the file, copy it to disk 1.

```
@ECHO OFF

REM ************************************************************
REM Edit the following values as necessary, then save to continue.
REM ************************************************************

REM Select your default Communications Method
SET COMMMETHOD=TCPIP
REM SET COMMMETHOD=NETBIOS

REM TCP/IP Values-Edit These To Be Values Valid for Your Shop
SET ADDR=9.82.1.300
SET SUBNET=255.255.255.0
SET ROUTE=9.82.1.301
SET DOMAIN=WASHINGTON.IBM.COM
SET NAMESERVER=9.82.1.303

REM ADSM Values-Edit These to Be Values Valid for Your Shop
SET NODENAME=MYNODENAME
SET TCPSERVERADDRESS=9.82.1.304
SET NETBIOSSERVERNAME=NETBADSM
SET TCPPORT=1500
```

Figure 48. SETUP.CMD File

B.8 RESCUE1.INI

RESCUE1.INI contains the initialization parameters for the CID Code Server, SERVICE.EXE. Figure 49 on page 278 shows the statements required to redirect three disks (C, D, and E), but you can add more if required.

Edit the values according to the ALIAS statements that are required. Be sure to define as many aliases as the number of disks you are redirecting.

To avoid initialization errors define aliases only for existing disks. The SERVICE program checks that the disk referenced in an alias statement is available.

Create a file called RESCUE1.INI and type in it the contents shown in Figure 49 on page 278 (even spaces are important). After you have created the file, copy it onto disk 1.

```
*
* RESCUE1.INI file  used by SERVICE.EXE
* ------------------------------------
* Edit the values or add more ALIAS sentences if required.
* Then, save to continue.
*
Name=RESCUE1
GroupName=yes
Adapter=0
MaxClients=1
Path=C:\
PermitWrite=no
MaxFiles=100
ClientWorkers=6
Alias=readwrite,single,DISKC,C:\
Alias=readwrite,single,DISKD,D:\
Alias=readwrite,single,DISKD,E:\
```

Figure 49. RESCUE1.INI File

Where to find more information

For more information about CID Code Server SERVICE.EXE and the initialization file, see *OS/2 Installation Techniques: The CID Guide, GG24-4295-00*. Appendix L describes the parameters used on the CID Code Server RESCUE1.INI file.

B.9 CONFIG.SYS

```
DOS=HIGH,UMB
DEVICE=HIMEM.SYS
DEVICE=EMM386.EXE NOEMS

FILES=50
BUFFERS=30
STACKS=9,256

DEVICEHIGH=A:\TCPDOS\PROTMAN.DOS /I:A:\TCPDOS
DEVICEHIGH=A:\TCPDOS\DOSTCP.SYS
DEVICEHIGH=A:\TCPDOS\IBMTOK.DOS
```

Figure 50. CONFIG.SYS File

B.10 AUTOEXEC.BAT

```
@echo off

set rtvmconv=0
set etc=a:\tcpdos

path=a:\;a:\tcpdos;

prompt=$p$g

rem **** TCP/IP Configuration ****

netbind

inet

route -fn
arp -dan

ifconfig nd0 129.33.160.90 netmask 255.255.255.0 up

route add default 129.33.160.254

echo on
```

Figure 51. AUTOEXEC.BAT File

B.11 DSM.OPT

```
Setting Options for the TCP/IP Communication Method
---------------------------------------------------
COMMMETHOD              TCPIP
TCPSERVERADDRESS        KINDU
TCPSERVERADDRESS        129.33.160.100
TCPPORT                 1500
TCPWINDOWSIZE           4
TCPBUFFSIZE             4

Setting Nodename
----------------

NODENAME                DOSWIN
```

Figure 52. ADSM Client Options (DSM.OPT) File

Appendix C. Special Notices

This publication is intended to help systems administrators put together and test a viable disaster recovery plan using ADSM client recovery. The information in this publication is not intended as the specification of any programming interfaces that are provided by ADSM. See the PUBLICATIONS section of the IBM Programming Announcement for ADSM for more information about what publications are considered to be product documentation.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM′s product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM′s intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

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 the IBM Director of Licensing, IBM Corporation, 500 Columbus Avenue, Thornwood, NY 10594 USA.

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, Dept. 600A, Mail Drop 1329, Somers, NY 10589 USA.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The information about non-IBM (″vendor″) products in this manual has been supplied by the vendor and IBM assumes no responsibility for its accuracy or completeness. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer′s ability to evaluate and integrate them into the customer′s operational environment. While each

item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Any performance data contained in this document was determined in a controlled environment, and therefore, the results that may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

Reference to PTF numbers that have not been released through the normal distribution process does not imply general availability. The purpose of including these reference numbers is to alert IBM customers to specific information relative to the implementation of the PTF when it becomes available to each customer according to the normal IBM PTF distribution process.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

IBM

The following terms are trademarks of other companies:

C-bus is a trademark of Corollary, Inc.

PC Direct is a trademark of Ziff Communications Company and is used by IBM Corporation under license.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Microsoft, Windows, and the Windows 95 logo
are trademarks or registered trademarks of Microsoft Corporation.

Other trademarks are trademarks of their respective companies.

Appendix D. Related Publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of some topics covered in this redbook. Other books listed cover related topics.

D.1 International Technical Support Organization Publications

For information on ordering these ITSO publications see “How to Get ITSO Redbooks” on page 287.

D.1.1 ADSM Redbooks

D.1.1.1 General Topics

Book Title	Publication Number
General Topics	
ADSM Concepts	SG24-4877
ADSM Version 2 Presentation Guide	SG24-4532
ADSM Advanced Implementation Experiences	GG24-4221
Using ADSM Hierarchical Storage Management	SG24-4631
Specific Server Books	
ADSM Server for Windows NT Configuration and Recovery Examples	SG24-4878
Getting Started with ADSM/6000	GG24-4421
ADSM for AIX: Advanced Topics	SG24-4601
AIX Tape Management	SG24-4705
ADSM/6000 on 9076 SP2	GG24-4499
ADSM for MVS: Recovery and Disaster Recovery	SG24-4537
ADSM for MVS: Using Tapes and Tape Libraries	SG24-4538
Getting Started with ADSM/2	GG24-4321
ADSM for OS/2: Advanced Topics	SG24-4740
Setting Up and Implementing ADSM/400	GG24-4460
ADSM/VSE Implementation Guide	SG24-4266
Specific Client Books	
Getting Started with ADSM NetWare Clients	GG24-4242
Getting Started with ADSM AIX Clients	GG24-4243
ADSM API Examples for OS/2 and Windows	SG24-2588
ADSM with Other Products	
Using ADSM to Back Up Databases	SG24-4335
Using ADSM to Back Up Lotus Notes	SG24-4534
HSM for NetWare: ADSM and AvailHSM Implementation	SG24-4713
Using ADSM to Back Up OS/2 LAN Server and Warp Server	SG24-4682
Backup, Recovery, and Availability with DB2 PE	SG24-4695

D.2 Redbooks on CD-ROMs

Redbooks are also available on CD-ROMs. **Order a subscription** and receive updates 2-4 times a year at significant savings.

CD-ROM Title	Subscription Number	Collection Kit Number
System/390 Redbooks Collection	SBOF-7201	SK2T-2177
Networking and Systems Management Redbooks Collection	SBOF-7370	SK2T-6022
Transaction Processing and Data Management Redbook	SBOF-7240	SK2T-8038
AS/400 Redbooks Collection	SBOF-7270	SK2T-2849
RS/6000 Redbooks Collection (HTML, BkMgr)	SBOF-7230	SK2T-8040
RS/6000 Redbooks Collection (PostScript)	SBOF-7205	SK2T-8041
Application Development Redbooks Collection	SBOF-7290	SK2T-8037
Personal Systems Redbooks Collection	SBOF-7250	SK2T-8042

D.3 ADSM Product Publications

Book Title	Publication Number
ADSM General Information	GH35-0131
ADSM V2 Installing the AIX Server and Administrative Client	SH35-0136
ADSM V2 for AS/400 Quick Start	GA32-0357
ADSM V2 for HP-UX Quick Start	GC35-0256
ADSM V2 Installing the MVS Server and Administrative Client	SH26-4043
ADSM V2 for OS/2 Quick Start	GC35-0231
ADSM V2 for Sun Solaris Quick Start	GC35-0262
ADSM V2 for VM Quick Start	GC35-0227
ADSM V2 for Windows NT Quick Start	GC35-0235
ADSM V2 for AIX Administrator's Guide	SH35-0134
ADSM V2 for AS/400 Administrator's Guide	SC35-0196
ADSM V2 for HP-UX Administrator's Guide	GC35-0257
ADSM V2 for OS/2 Administrator's Guide	GC35-0232
ADSM V2 for Sun Solaris Administrator's Guide	GC35-0263
ADSM V2 for MVS Administrator's Guide	SH26-4039
ADSM V2 for VM Administrator's Guide	GC35-0228
ADSM V2 for Windows NT Administrator's Guide	GC35-0236
ADSM V2 for AIX Administrator's Reference	SH35-0135
ADSM V2 for AS/400 Administrator's Reference	SC35-0197
ADSM V2 for HP-UX Administrator's Reference	GC35-0258
ADSM V2 for MVS Administrator's Reference	SH26-4040
ADSM V2 for OS/2 Administrator's Reference	GC35-0233
ADSM V2 for Sun Solaris Administrator's Reference	GC35-0264
ADSM V2 for VM Administrator's Reference	GC35-0229
ADSM V2 for Windows NT Administrator's Reference	GC35-0237
ADSM V2 for MVS DRM Administrator's Guide and Reference	GC35-0238
ADSM V2 Messages	SH35-0133
ADSM V2 Device Configuration	SH35-0137

Book Title	Publication Number
ADSM V2 Installing the Clients	SH26-4049
ADSM V2 AFS/DFS Backup Clients	SH26-4048
ADSM V2 Using the UNIX HSM Clients	SH26-4030
ADSM V2 Using the UNIX Backup-Archive Client	SH26-4052
ADSM V2 Using the OS/2 Backup-Archive Client	SH26-4053
ADSM V2 Using the DOS Backup-Archive Client	SH26-4054
ADSM V2 Using the Microsoft Windows Backup-Archive Clients	SH26-4056
ADSM V2 Using the Novell NetWare Backup-Archive Client	SH26-4055
ADSM V2 Using the Apple Macintosh Backup-Archive Client	SH26-4051
ADSM V2 Using the Lotus Notes Backup Agent	SH26-4047
ADSM V2 Using the Application Programming Interface	SH26-4002
ADSM V2 Reference Cards for the Backup-Archive Clients	SX26-6013

D.4 ADSM Online Product Library

All of the ADSM publications are available in online readable format on the CD-ROM listed below. The ADSM library is also available on the following CD-ROMs: These books can also be ordered in softcopy format on CD-ROM:

CD-ROM Title	Publication Number
ADSM Online Product Library	SK2T-1893
MVS Base Collection Kit	SK2T-0710
VM Base Collection Kit	SK2T-2067
AS/400 Base Collection Kit	SK2T-2171

How to Get ITSO Redbooks

This section explains how both customers and IBM employees can find out about ITSO redbooks, CD-ROMs, workshops, and residencies. A form for ordering books and CD-ROMs is also provided.

This information was current at the time of publication, but is continually subject to change. The latest information may be found at URL http://www.redbooks.ibm.com.

How IBM Employees Can Get ITSO Redbooks

Employees may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **PUBORDER** — to order hardcopies in United States
- **GOPHER link to the Internet** - type GOPHER.WTSCPOK.ITSO.IBM.COM
- **Tools disks**

  To get LIST3820s of redbooks, type one of the following commands:

  ```
  TOOLS SENDTO EHONE4 TOOLS2 REDPRINT GET SG24xxxx PACKAGE
  TOOLS SENDTO CANVM2 TOOLS REDPRINT GET SG24xxxx PACKAGE (Canadian users only)
  ```

  To get lists of redbooks:

  ```
  TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET ITSOCAT TXT
  TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET LISTSERV PACKAGE
  ```

  To register for information on workshops, residencies, and redbooks:

  ```
  TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ITSOREGI 1996
  ```

  For a list of product area specialists in the ITSO:

  ```
  TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ORGCARD PACKAGE
  ```

- **Redbooks Home Page on the World Wide Web**

  http://w3.itso.ibm.com/redbooks

- **IBM Direct Publications Catalog on the World Wide Web**

  http://www.elink.ibmlink.ibm.com/pbl/pbl

  IBM employees may obtain LIST3820s of redbooks from this page.

- **REDBOOKS category on INEWS**
- **Online** — send orders to: USIB6FPL at IBMMAIL or DKIBMBSH at IBMMAIL
- **Internet Listserver**

  With an Internet e-mail address, anyone can subscribe to an IBM Announcement Listserver. To initiate the service, send an e-mail note to announce@webster.ibmlink.ibm.com with the keyword subscribe in the body of the note (leave the subject line blank). A category form and detailed instructions will be sent to you.

How Customers Can Get ITSO Redbooks

Customers may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **Online Orders** (Do not send credit card information over the Internet) — send orders to:

	IBMMAIL	**Internet**
In United States:	usib6fpl at ibmmail	usib6fpl@ibmmail.com
In Canada:	caibmbkz at ibmmail	lmannix@vnet.ibm.com
Outside North America:	dkibmbsh at ibmmail	bookshop@dk.ibm.com

- **Telephone orders**

United States (toll free)	1-800-879-2755
Canada (toll free)	1-800-IBM-4YOU
Outside North America	(long distance charges apply)
(+45) 4810-1320 - Danish	(+45) 4810-1020 - German
(+45) 4810-1420 - Dutch	(+45) 4810-1620 - Italian
(+45) 4810-1540 - English	(+45) 4810-1270 - Norwegian
(+45) 4810-1670 - Finnish	(+45) 4810-1120 - Spanish
(+45) 4810-1220 - French	(+45) 4810-1170 - Swedish

- **Mail Orders** — send orders to:

IBM Publications	IBM Publications	IBM Direct Services
Publications Customer Support	144-4th Avenue, S.W.	Sortemosevej 21
P.O. Box 29570	Calgary, Alberta T2P 3N5	DK-3450 Allerød
Raleigh, NC 27626-0570	Canada	Denmark
USA		

- **Fax** — send orders to:

United States (toll free)	1-800-445-9269
Canada	1-403-267-4455
(+45) 48 14 2207 (long distance charge)	Outside North America

- **1-800-IBM-4FAX (United States)** or **(+1)001-408-256-5422 (Outside USA)** — ask for:

  Index # 4421 Abstracts of new redbooks
  Index # 4422 IBM redbooks
  Index # 4420 Redbooks for last six months

- **Direct Services** - send note to softwareshop@vnet.ibm.com
- **On the World Wide Web**

Redbooks Home Page	http://www.redbooks.ibm.com
IBM Direct Publications Catalog	http://www.elink.ibmlink.ibm.com/pbl/pbl

- **Internet Listserver**

  With an Internet e-mail address, anyone can subscribe to an IBM Announcement Listserver. To initiate the service, send an e-mail note to announce@webster.ibmlink.ibm.com with the keyword subscribe in the body of the note (leave the subject line blank).

IBM Redbook Order Form

Please send me the following:

Title	Order Number	Quantity

First name Last name

Company

Address

City Postal code Country

Telephone number Telefax number VAT number

- Invoice to customer number
- Credit card number

Credit card expiration date Card issued to Signature

We accept American Express, Diners, Eurocard, Master Card, and Visa. Payment by credit card not available in all countries. Signature mandatory for credit card payment.

DO NOT SEND CREDIT CARD INFORMATION OVER THE INTERNET.

Index

Numerics

A

B

C

O

P

R

S

V

W

Printed in U.S.A.