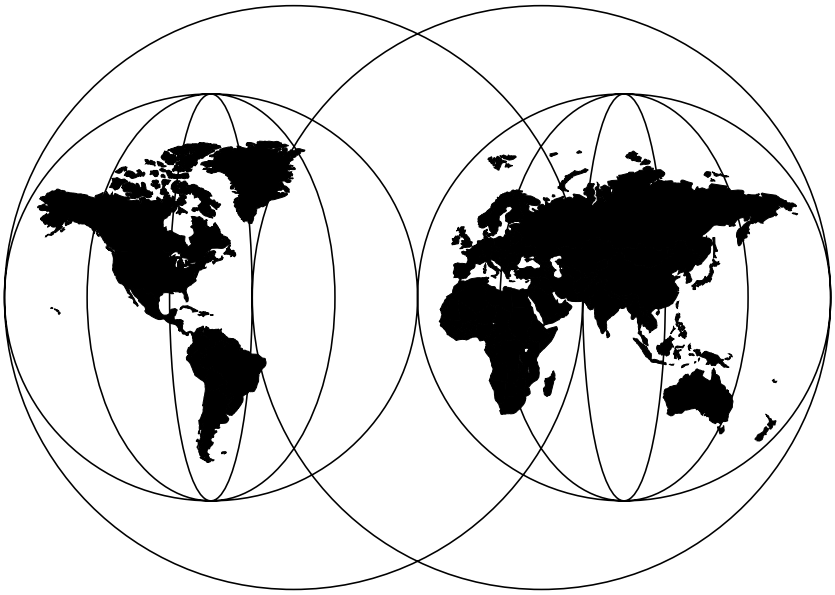
IBM

AIX and Windows NT Solutions for Interoperability

Laurent Vanel, Steve Gardner, Praben Prima, Simon Robertson, Oreste Villari



International Technical Support Organization

http://www.redbooks.ibm.com

SG24-5102-00

SG24-5102-00

International Technical Support Organization

AIX and Windows NT
Solutions for Interoperability

May 1998

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 321.

First Edition (May 1998)

This edition applies to AIX Version 4, Novell Network Services Version 4.1 for AIX, and AIX Connections 4.1.6 for AIX Version 4.

Comments may be addressed to:
IBM Corporation, International Technical Support Organization
Dept. JN9B Building 045 Internal Zip 2834
11400 Burnet Road
Austin, Texas 78758-3493

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

Tables

Preface

This redbook is intended to help you understand how to integrate your AIX computer into an NT environment, and how to share AIX resources with your Windows NT computer. We have focused our description on the key areas, which are disk and printer sharing.

The products described in this book are Samba Version 1.9.18, AIX Connections Version 4.1.6, Novell NetWare Services Version 4.1, Advanced Server UNIX Version 4.0 and TotalNet Version 5.2. These products were chosen because of their popularity with customers and their availability from IBM.

Each chapter focuses on one of these products to help you decide which one is the most appropriate for your specific needs. The second part of each chapter is a step by step approach to the installation, configuration and customization of the software.

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 Austin Center.

Steve Gardner is an Information Technology Specialist at the International Technical Support Organization, Austin Center. He has been with IBM for 14 years, holding a variety of hardware, software and network support positions. Before joining the ITSO one and one-half years ago, Steve worked as the AIX system administrator and Webmanager in the Somerset Design Center, the joint Apple/IBM/Motorola PowerPC project.

Praben Prima is an AIX Software Support Specialist in Indonesia. He has been with IBM for seven years, and in the last two years he has specialized in AIX and networking. His areas of expertise include HACMP and SP2. He holds a degree in Telecommunication Engineering from ITS Institute of Technology, Surabaya, Indonesia. He has written extensively on AIX system management and problem determination.

Simon Robertson is an RS/6000 specialist in the United Kingdom and has worked with IBM for four and one-half years. He holds a BSC degree in Technology and Business Studies from Strathclyde University, Glasgow. His areas of expertise include AIX and Windows NT.

Laurent Vanel is an AIX specialist at the International Technical Support Organization Austin Center. He is from Paris, France, where he joined IBM in February 1990, at the same time the first RS/6000s were announced. Since then he has provided AIX support to both field engineers and customers.

Oreste Villari is an AIX System Specialist in Genoa, Italy. He has 10 years experience in the AIX area. He holds a degree in Mechanical Engineering from Genoa University. His areas of expertise include RISC technology, the AIX operating system and LAN/WAN environments. He has also written on e-mail in a client/server heterogeneous environment.

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

John Weiss
International Technical Support Organization Austin Center

Ed Ponzini
AIX Architecture

Jay Ashford
AIX Architecture

Rakesh Sharma
IBM RISC System Division, Austin

Denise Genty
AIX NetWare Development

Comments Welcome

Your comments are important to us!

We want our redbooks to be as helpful as possible. Please send us your comments about this or other redbooks in one of the following ways:

- Fax the evaluation form found in “ITSO Redbook Evaluation” on page 339 to the fax number shown on the form.
- Use the electronic evaluation form found on the Redbooks Web sites:

  For Internet users `http://www.redbooks.ibm.com`
  For IBM Intranet users `http://w3.itso.ibm.com`

- Send us a note at the following address:

  `redbook@vnet.ibm.com`

Chapter 1. Introduction

The purpose of this chapter is to describe the network environment used by the different products covered in this redbook. This chapter also includes definitions for common Windows NT terms used throughout the book.

1.1 The Network Environment

It is not the intention of this publication to cover the installation of AIX and Windows NT or to demonstrate how to configure TCP/IP on these systems.

Figure 1 describes the network topology used in this book and shows the different systems installed.

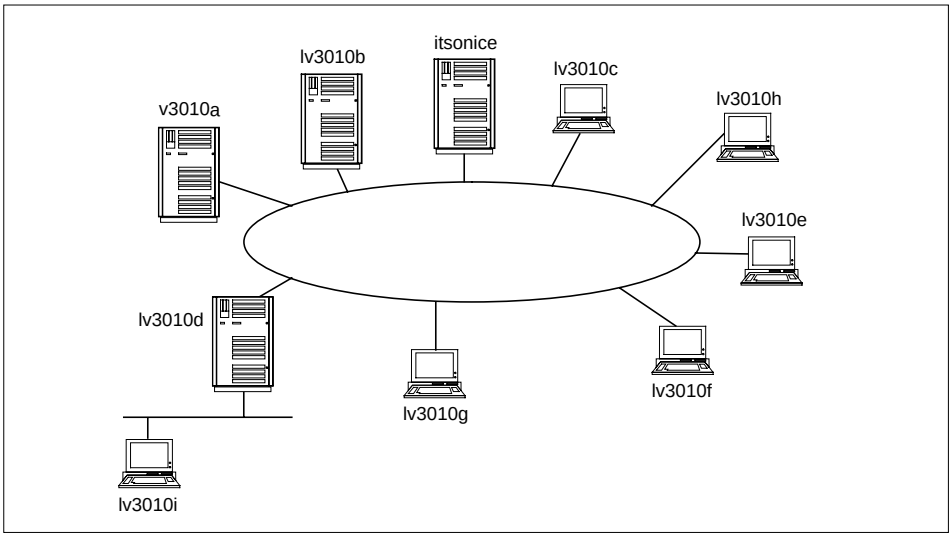


Figure 1. Topology of the Network for This Document

1.1.1 Names and Roles of the Systems

The products covered in this redbook can run on most of the RS/6000s. However, we decided to install the products on similar platforms so we could compare them. The RS/6000s mentioned in his redbook are:

lv3010a — A 43P (7248-132) running AIX 4.2.1 and Advanced Server for UNIX, Version 4.0, from Group Bull.

lv3010b — A 43P (7248-132) running AIX 4.2.1 and AIX Connections Version 4.1.6.

lv3010c	A 43P (7248-132) running AIX 4.2.1 and TotalNET Advanced Server from Syntax, Version 5.2.
lv3010d	A 43P (7248-132) running AIX 4.2.1 and Novell Network Services Version 4.1.
outshines	A 7025-F40 running AIX 4.3 and Samba Version 1-9.18p1.
lv3010e, lv3010f, lv3010g	PCs (Pentium 166 MMX with 64 MB memory) running Windows NT Server.
lv3010h, lv3010i, lv3010k	PCs (Pentium 166 MMX with 32 MB memory) running Windows NT workstation.

1.2 Definitions of Common Terms

Throughout this redbook we use terms related to networking environments in the Windows NT world. For those of you who are not familiar these terms, you will find the following definitions useful.

1.2.1 Domains

A domain is a logical grouping of network servers and other computers that share common security and user account information. The group of servers and other computers do not have to be in the same physical location or be connected over the same physical connection. It is from within the domain that administrators create user accounts. Each account that is created includes user information, group memberships and a security policy.

Within the domain there is a primary domain controller (PDC). A master copy of the directory database that contains all security and user account information is stored in the PDC. The directory database is used for user logon validation. The domain model allows a user to log on any machine in the domain since the validation is carried out at the PDC. In addition, network users are able to connect to multiple servers with a single network logon and access the available resources.

There is a second type of domain controller, a backup domain controller (BDC). The BDC maintains a copy of the directory database, which is kept up to date with the master database on the PDC. The PDC sends signals to the BDC at specified intervals to request changes from the PDC. If there is an immediate requirement for BDCs to be updated with directory changes (the default timing of updates is every five minutes), the synchronization can be forced. BDCs also authenticate user logons. Within a Domain, there can be multiple BDCs.

Windows NT servers that are neither PDCs or BDCs can be member servers that provide resources to the network, such as files, printers or applications.

1.2.2 Trust Relationships

For small organizations, a single domain may be all that is required to run the Windows NT network. In larger organizations, multiple domains may be implemented so that groups of systems and users are controlled with more granularity. For example, a company may have one domain for the marketing department and one domain for the finance department. To allow users in one domain to access resources in a another domain, a Trust Relationship must be established. There are two types of Trust Relationships. In a one-way Trust Relationship, one domain trusts users in another domain to access it's resources. In a two-way Trust Relationship, users in each domain are trusted to access resources in each others domains (a two-way trust relationship is two one-way trusts).

Using Trust Relationships, users can access resources from other domains as if they were accessing resources in their own domain.

Trust Relationships can become complex when many domains are used and you want all domains to trust each other. This is because a Trust Relationship has to be set up on every server for every other server (for example, if an organization had 10 domains, 90 Trust Relationships would have to be established and maintained to provide full access to all members in all domains).

1.2.3 Workgroups

A workgroup is a logical collection of workstations and servers that do not belong to a domain. In a workgroup, each computer stores its own copy of user and group account information. Therefore, in workgroups, users can only log directly onto machines on which they have accounts. Workgroup members are able to view and use resources on other systems. To do this, resources are shared in the workgroup and network users are validated by the machine owning the resource (for example, a directory or printer).

Chapter 2. Using the Base Operating Systems

Perhaps your need for AIX and Windows NT interoperability is minimal, for instances such as occasional file transfers, a special print job on a specific printer or a remote connection to manage the AIX server. This chapter summarizes what you can do between AIX and Windows NT machines installed only with the core operating systems.

2.1 Remote Connection to the AIX Machine

Assume that you have a Windows NT workstation and you want to access a remote AIX machine. It's very simple, since the `telnet` command is included in the Windows NT operating system (usually in C:\WINNT\system32) and the telnetd counterpart daemon is standard in AIX. Just start the `telnet` command from your Windows NT workstation, either from a DOS command-prompt or from any shortcut.

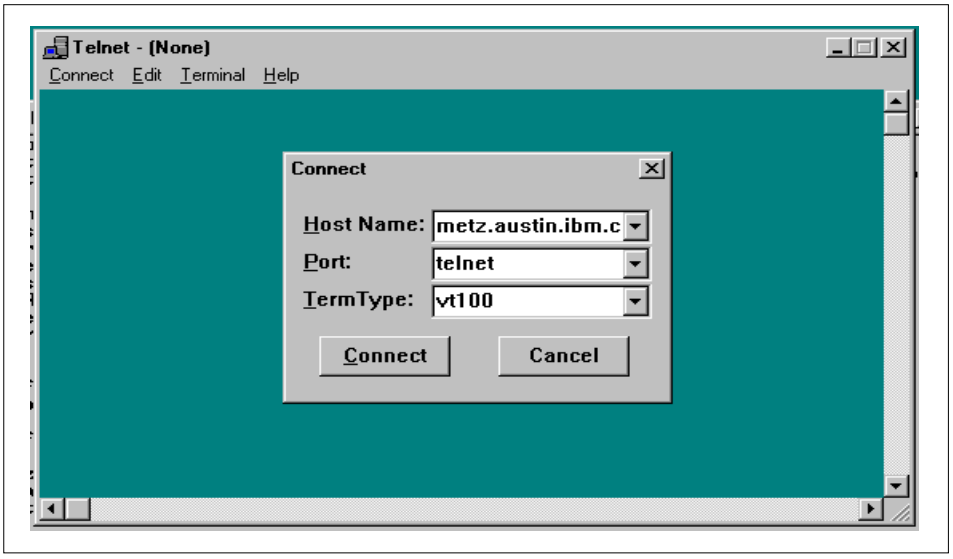


Figure 2. The telnet Command

As you can in Figure 2, you can select the type of terminal you want to use (you have the choice of `vt100`, `ansi`, `DEC-VT100`, `VT100` or `ANSI`). Select the one for which you have an entry in your terminfo file; for AIX. `vt100` is a good choice. You can also select the port to reach on the remote host. The default, `telnet`, should be used. You can now start any character-based applications

running on the AIX machine. Some third-party products offer a telnetd daemon for Windows NT that gives you a DOS command prompt.

2.2 File Transfer

To transfer files between AIX and Windows NT, the `ftp` command is the answer. The client command is available on both AIX and Windows NT. The default location for the `ftp` command is C:\WINNT\system32.

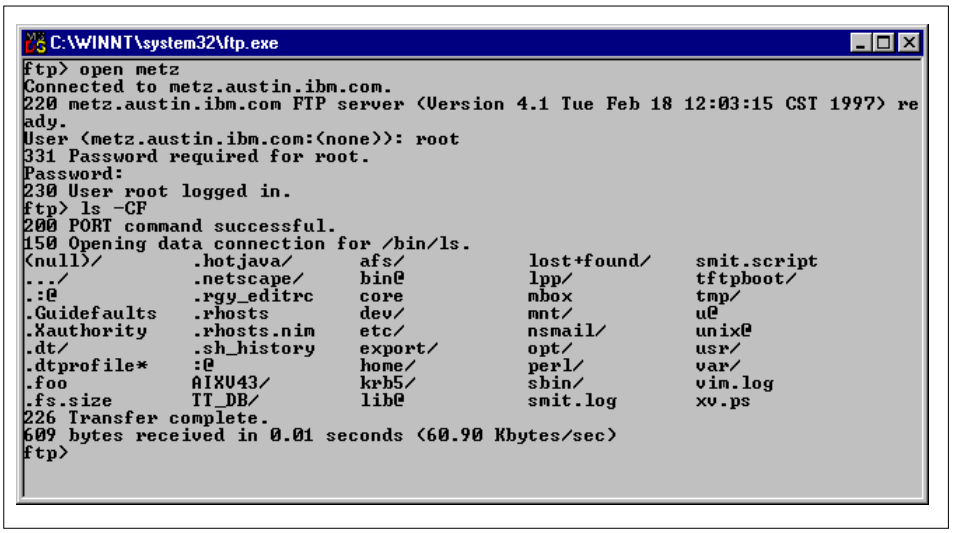


Figure 3. The ftp Command

The server part for ftp (ftpd) is standard in AIX and is a part of the Microsoft Internet Information Server package. On Windows NT, you can customize the ftpd service by starting the Internet Service Manager application.

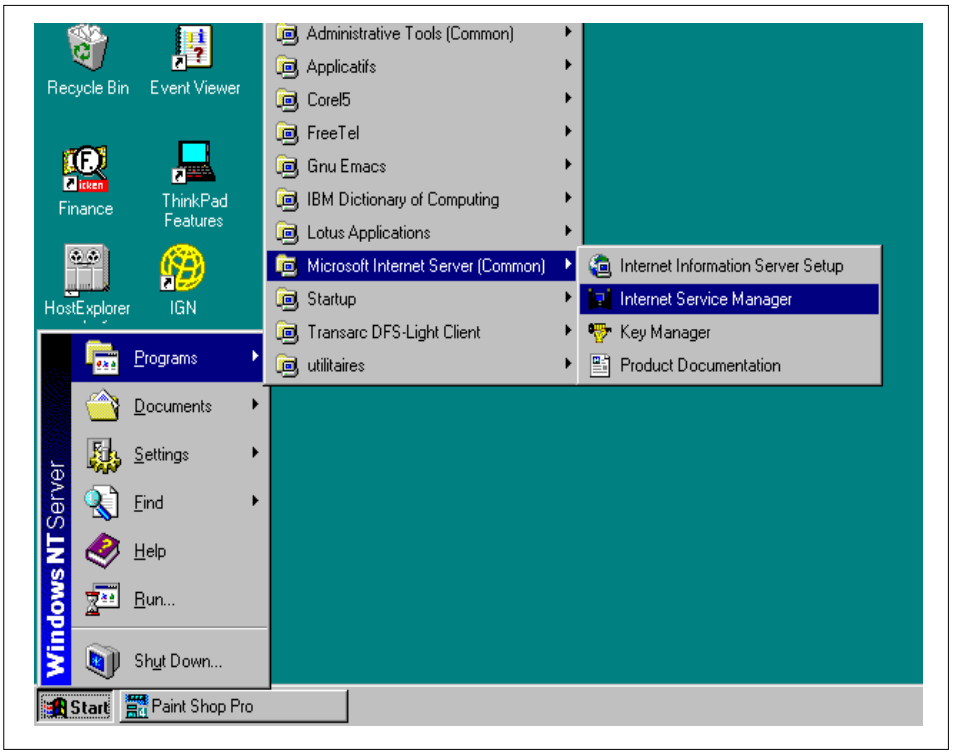


Figure 4. Starting the Internet Service Manager

Of the many elements you can change, the following list details some of the most useful elements:

- The TCP port (defaults is 21).
- The connection time-out (default is 900).
- The maximum number of connections (default is 1000).
- The welcome, exit and too many connections messages (default is empty).
- The logging of the connections.
- The filtering of the connections (you can restrict the access to your ftp server based on the IP address of the client).
- The creation of aliases for commonly accessed directory. The Figure 5 shows how to create an alias, /informations, for the directory D:\laurent\information_6000, and how to make this directory read-only.

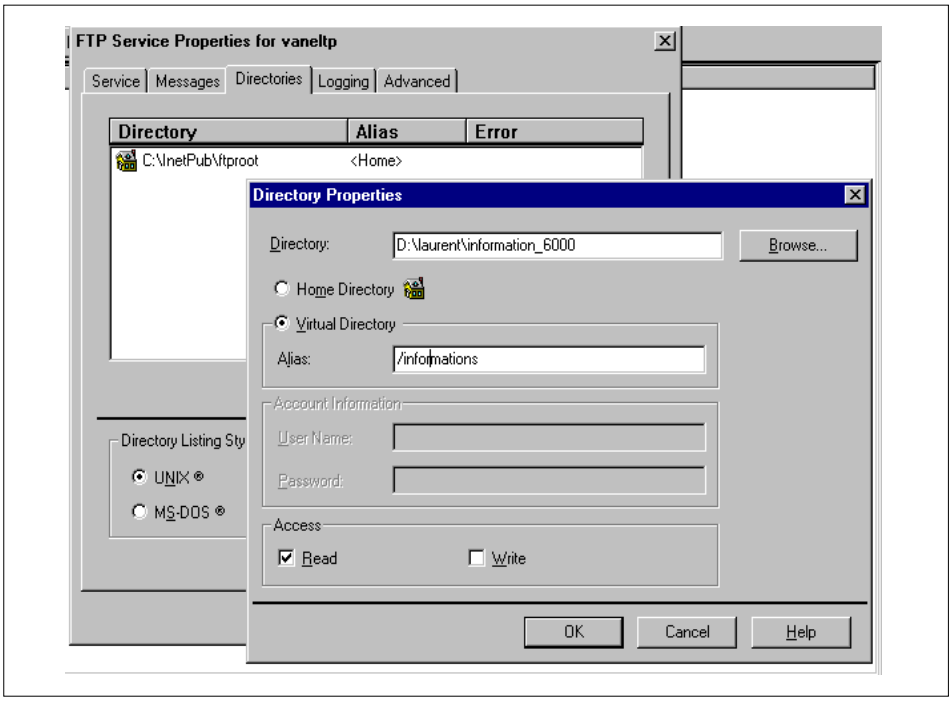


Figure 5. Creating an Alias for the ftp Service

2.3 Remote Printing

Another remote resource you can use is a printer. Either you are connected to your NT workstation and you want to use the printer attached to the AIX machine, or you are connected to an AIX machine and want to use the printer attached to a Windows NT machine. Our answer to both scenarios is to use the LPR/LPD commands. Let's see how to configure your systems to do that.

2.3.1 Using a Remote Printer Attached to an AIX Machine

In the first case, you are connected to an Windows NT workstation and you want to access a printer attached to an AIX machine. The LPR/LPD commands are installed by default on AIX machines but not on Windows NT machines. So our first step is to install the necessary software. The LPR command is included in the Microsoft TCP/IP printing service. If this service is not installed on your system, right-click on the Network Neighborhood icon and select **Properties**. Figure 6 shows you how to check if this service is installed (if you don't see this service, click on the **Add...** button and select its entry on the list).

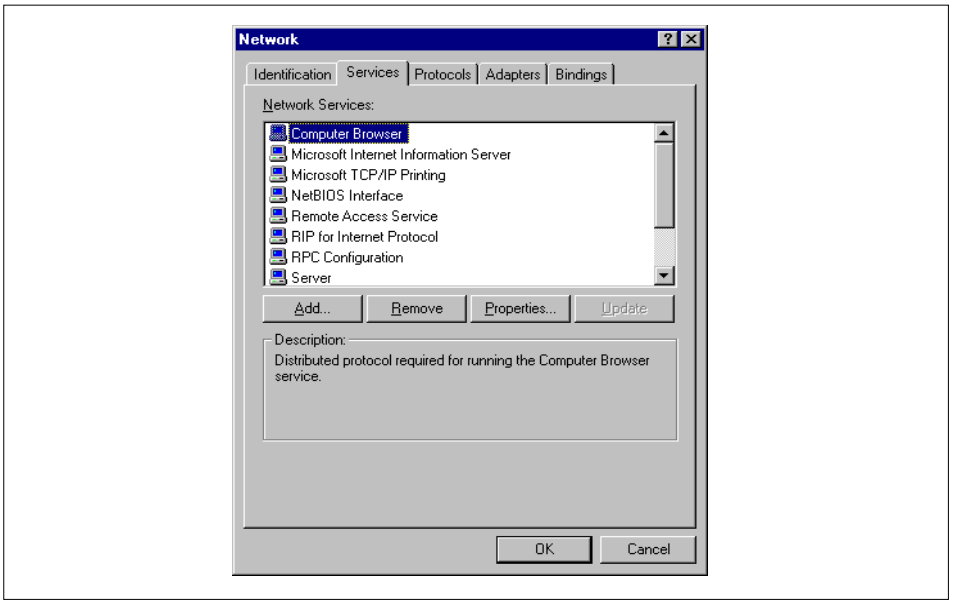


Figure 6. The Microsoft TCP/IP Printing Service Must Be Installed

Once this service is added to your machine you can add a new printer (of course you need the proper authorizations to do so). Double-click on the **My Computer** icon, select the **Printers** panel and double-click on the **Add Printer** icon. The Add printer Wizard is launched to assist you in this task. Select a local printer, and the next panel requires that you select a port. Click on the **Add port** button, and a new window appears. If you followed the previous steps, one of the choices is **LPR port**; select this item (if it does not appear, you must install the Microsoft TCP/IP service). You are then prompted for the name or address of the server to which the printer is attached and the name of the remote queue. Figure 7 on page 10 summarizes these steps. The end of the configuration process is the same as adding a local or remote printer. You can now use this new print queue.

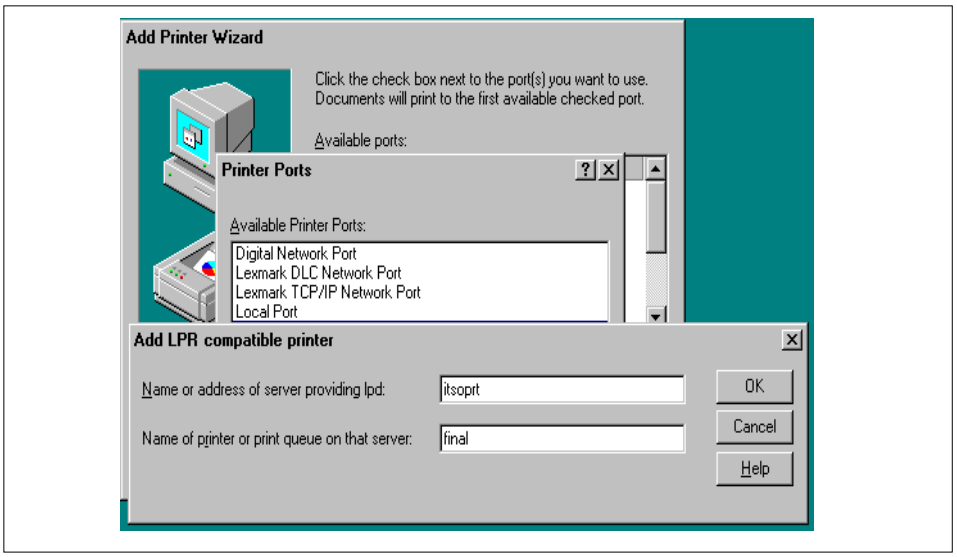


Figure 7. Adding a Queue That Uses a Remote Printer

Of Course on the AIX machine you must authorize the Windows NT machine to use the lpd service. In order to do that you must add an entry to the /etc/lpd/hosts file for this machine. You can also use SMIT (with fast path mkhostslpd) to perform this action.

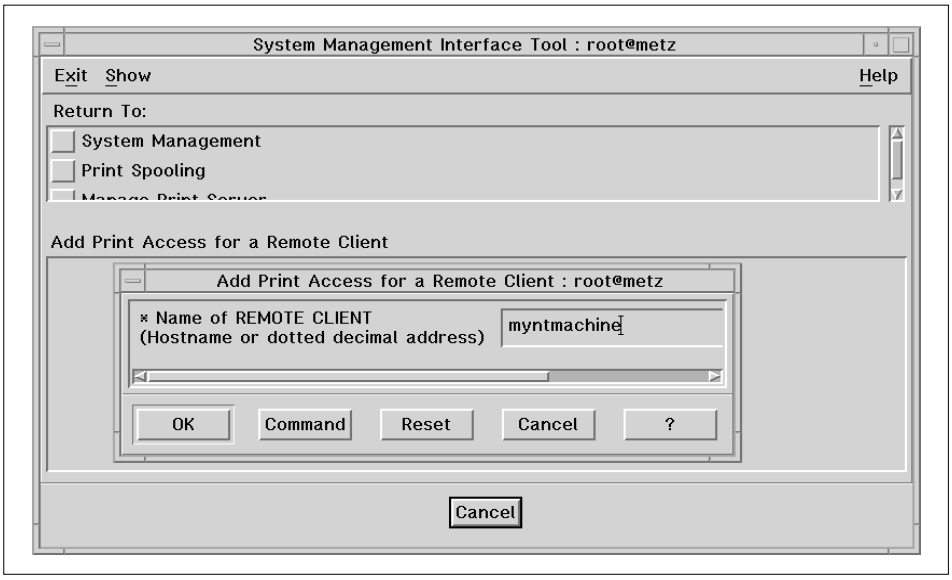


Figure 8. Authorizing the NT Machine to Use the lpd Service

2.3.2 Using a Remote Printer Attached to an NT Machine

First, let's add a new queue on the AIX machine. There are several tools that allow you to perform this task (such as SMIT, xprintm or the new Web system management). Whatever tool you use, you must fill-out a window similar to the one below.

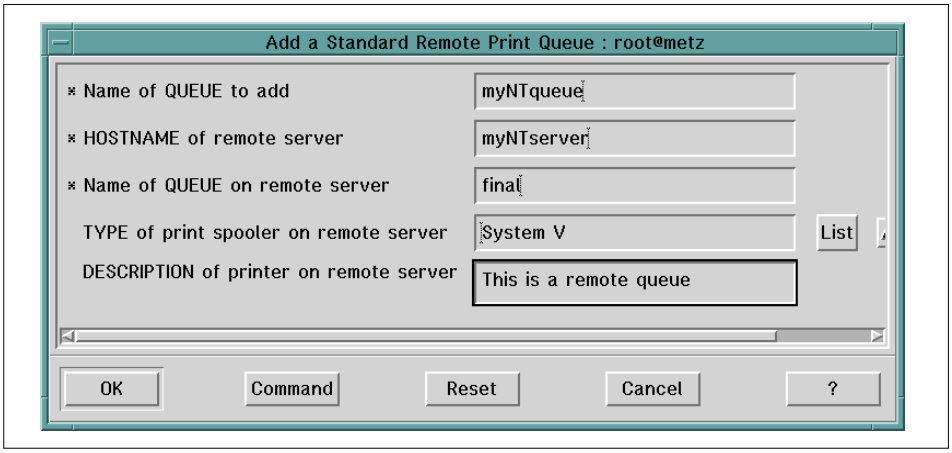


Figure 9. Adding a Remote Queue on an AIX Machine

Once this step is finished you are ready to print, though you have to start the LPD service on your NT machine. This is done in the server manager window of Windows NT. To access this application, open the control panel and double-click on the **Service** icon, scroll down to find the TCP/IP Print Server entry and configure it to be started (either now or both now and after reboot). You can now use this print queue from your AIX workstation.

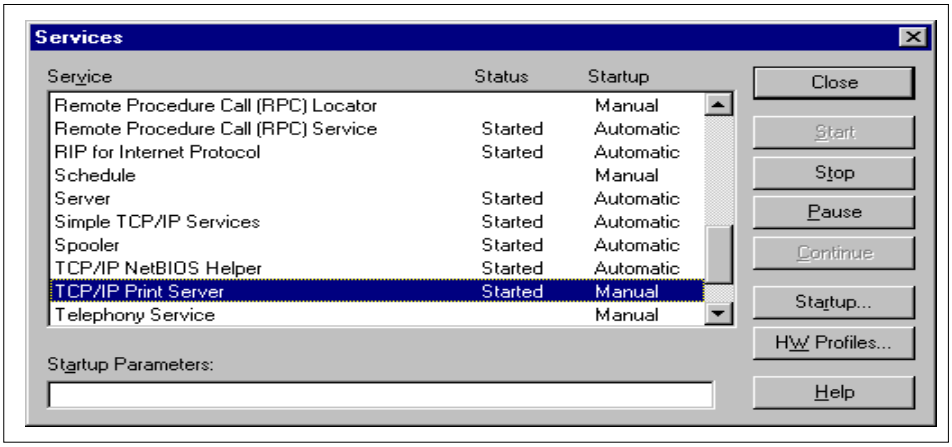


Figure 10. Starting the LPD Service on the NT Machine

To have more integration between your AIX and NT machines, let's start with TotalNET from Syntax.

Chapter 3. TotalNET Advanced Server

In this chapter we discuss the connection setup between Windows NT and AIX using **TotalNET Advanced Server** (TAS).

We also discuss how TAS provides services such as file or printer service to Windows NT clients. In this case we use AIX 4.2.1 with TAS Version 5.2 and Windows NT 4.

3.1 TAS Overview

In this section we discuss the product and some of the terms used in this chapter.

3.1.1 The History of TAS

TAS is a product from Syntax, Inc., based in Federal Way, Washington. Since 1983, Syntax, Inc. has produced LAN software products to support the growing client/server market.

Syntax's flagship product, TotalNET Advanced Server (TAS), was released in 1992. TAS enables AIX systems to be used as servers and provides services to clients running popular operating systems such as OS/2, Windows 95, Windows 3.x, Windows for Workgroups, Windows NT, LAN Manager, NetWare or Macintosh to share resources such as files and printers.

With this capability you can have AIX applications and services transparently available to LAN users, and share files and printers previously defined in AIX, without modifying the clients' system. This reduces the costs and time spent administering and supporting the environment.

On January 5, 1998, IBM licensed TAS and will ship the product in future releases of AIX in a bonus pack. The bonus pack product can be used for one client, and customers have the opportunity to evaluate it. If customers intend to buy the product they can contact Syntax directly through the nearest representative office.

3.1.2 Using TAS

In many environments, managing a client/server is not an easy task. Many companies are forced to adopt a PC-based NFS solution to share information between PC and UNIX servers. In some cases, client computers must use multiple protocols. Many environments already have several separate LANs,

and integrating them into a suitable and reliable working condition is costly and complicated.

One solution is to simplify the network itself, but this takes extra effort. A software solution that provides interoperability in a complex environment and overcomes the differences among clients would be ideal.

TAS has this capability. It includes server software that supports PC clients using LAN Manager or other network operating systems, NetWare and Macintosh clients, and allows users on the network to share resources such as files, data, and printers without changing their clients' configuration.

TAS can also work in WAN environments using routers. However, in this chapter we explain how to implement TAS using AIX and Windows NT in a LAN environment only.

3.1.3 Brief Description

In this section we discuss the basic structure of TAS and its services.

3.1.3.1 Realms

TAS is packaged in three realms. A realm is basically a set of software that gives services to different types of clients. There are three realms:

- **LM-NT-OS/2 realm** — The realm for LAN Manager, Windows NT, Windows 95, and OS/2 clients running NetBIOS over TCP/IP or NetBIOS over NetBEUI transports.
- **NetWare realm** — The realm for NetWare clients running the IPX/SPX transport.
- **AppleTalk realm** — The realm for Macintosh clients running the AppleTalk transport.

  To provide services to Windows NT clients, you need to have the LM-NT-OS/2 realm installed.

3.1.3.2 TNAS

To administer TAS, we will use TotalNET Administration Suite (TNAS). It is a task-oriented graphical administration and configuration environment for the system administration, licensing and configuration of TotalNET products. TNAS is an HTML-based menu and dialog system that allows end users without extensive AIX administration skills to take advantage of AIX capabilities.

TNAS uses Java applets. You can see that whenever you put your cursor on the TNAS icon, it gives a message: `Need Java applets to use`. That is why we need to use a Web browser that supports Java.

3.1.3.3 Services

The power of TAS is the ability to provide services to heterogeneous LAN clients without changes or additions to the clients. TAS provides three services:

- File service

  File service gives us the capability to share certain directories or file systems with the clients. This is done by creating volumes, which we will discuss later in this section. We also have the flexibility to define a user's permission to the file service.

- Printer service

  TAS printer service is done through file service. We can make AIX printers available to the clients by defining the printer to the file service.

- Terminal service

  If needed, TAS also provides terminal service. It allows a client's terminal emulator programs to connect to AIX using NetBIOS as a transport. We need a terminal emulator that supports NetBIOS, such as Kermit.

3.1.3.4 TNHOME directory

All TAS programs are placed in directory /var/totalnet, which is identified by the $TNHOME variable. You will have to add this information in your /etc/environment file. You also need to specify /var/totalnet/usr/bin and /var/totalnet/usr/sbin in your PATH variable.

3.2 Licensing Policy

As mentioned before, TAS will be distributed by IBM in a bonus pack. Customers can then evaluate the product for a one-client configuration. If TAS suits their needs, they can purchase the product by contacting Syntax, and getting the license key. This key is to be used with a specific number of clients.

Customers can contact Syntax in several ways:

- Contact Syntax Inc. headquarters in the United States at (253)-838-2626. Syntax will then refer customers to a local representative.
- Sending e-mail to:

sales@syntax.com

Through e-mail, potential customers can ask general questions about the product.

- At the Syntax Web site (www.syntax.com), customers can find a Partners section that lists all international distributors and resellers. This is updated regularly and includes phone, fax, and e-mail information, as well as links to their site.

3.3 System Requirements

There are several system requirements when using TAS 5.2.

3.3.1 Server Hardware Requirements

TAS can operate in any machine that runs AIX. However, it won't work in a diskless or dataless machine, because it functions as a server. You will need to have a token-ring, Ethernet, or FDDI adapter installed in your server.

3.3.2 Server Software Requirements

The following software must be installed on your server to run the current version of TAS:

- AIX 4.1.4 or later

bos.net.tcp.server 4.1.3.0	TCP/IP server
bos.txt.tfs 4.1.3.0	Text formatting services
bos.rte.streams 4.1.4.3	Streams library
bos.rte.tty 4.1.4.10	Base TTY support and commands
bos.data 4.1.4.0	Base operating system data

- PTF for AIX 4.1.4

U443346	For bos.rte.tty 4.1.4.10
U441953	For bos.rte.streams 4.1.4.3

- Web browser with support for tables, forms, Java, and JavaScript (for example, Netscape Navigator 3.0 or higher and Microsoft Internet Explorer 3.0.1 or higher)
- License use management client software
- Disk space of approximately 35 MB in /usr

3.3.3 Client Hardware Requirements

All clients must have the following installed:

- Ethernet
- Token-ring

3.3.4 Client Software Requirements

Client software requirements include a LAN requester, such as:

- IBM's LAN Server Version 3.0 or higher
- Microsoft's LAN Manager
- Microsoft's Windows for Workgroups
- Microsoft Windows NT

We have Microsoft Windows NT 4 installed on our PC.

3.4 TAS Installation

Before doing the installation, please make sure you have met the system requirements.

TAS includes the following packages:

- TAS.server.admin 5.2.0.0
- TAS.server.doc 5.2.0.0
- TAS.server.com 5.2.0.0
- TAS.server.lmserver 5.2.0.0
- TAS.server.macserver 5.2.0.0
- TAS.server.man 5.2.0.0
- TAS.server.nwserver 5.2.0.0

TAS 5.2 cannot operate on the same system with earlier versions of TAS, TAS components, or TNclient. If your system contains any of these, begin by upgrading them as instructed in "Upgrading Earlier Versions of TAS" on page 20.

Notes

Before installing TAS, be sure to configure TCP/IP and have your hostname set. TAS will use the hostname of your workstation to set up service names.

If you have AIX Connections installed on your system, TAS installation will fail with a message, `connect.server has not been installed and could not be found in the media`. Simply remove the AIX Connections filesets and proceed with TAS installation.

Before you continue with the installation, take a few steps to ensure that you have a correct DLPI configuration, as explained in the following section.

3.4.1 DLPI Configuration

DLPI is the data link provider interface that determines which device driver to use in your configuration. Those familiar with AIX Connection will notice that the installation process does this DLPI configuration automatically. TAS does not have the capability to change this automatically, so we will have to do it manually.

Follow these steps to configure DLPI by editing the files /etc/dlpi.conf and /etc/pse.conf:

1. Uncomment the lines for the interface you want to configure. For example, you need to remove pound sign (#) from the beginning of the third line to uncomment the token-ring driver, in addition to the already-uncommented Ethernet driver. Since we use token-ring, we remove the # from the third line, which is for the token-ring driver. This code comes from the /etc/dlpi.conf file.

```
d+      dlpi    en      /dev/dlpi/en    # streams dlpi ethernet driver
#d+     dlpi    et      /dev/dlpi/et    # streams dlpi 802.3 driver
d+      dlpi    tr      /dev/dlpi/tr    # streams dlpi token ring driver
#d+     dlpi    fi      /dev/dlpi/fi    # streams dlpi FDDI driver
```

2. The following shows you the lines you should uncomment in the /etc/pse.conf file:

```
d+      stddev  echo    /dev/echo       # what-u-write-is-what-u-read
d+      stddev  nuls    /dev/nuls       # streams version of /dev/null
d       spx                             # streams "pipe multiplexor"
m       sc                              #streams config list (scls) module
```

3. Reboot your system for these changes to take effect.

3.4.2 Installation Steps

The AIX installation program extracts the TAS software package from the distribution media, sets the ownership and permission mode of the files, and moves them to the appropriate directories. This example of the installation process shows the installation of all packages. You can install through the usual TAS installation method from the command line or with SMIT.

3.4.2.1 Installation Using SMIT

Follow these steps to install TAS using SMIT:

1. Log in as **root** and enter SMIT:

   ```
   smit install_latest
   ```

2. At the **Install and Update from LATEST Available Level** panel, enter the INPUT device field:

   ```
   /mntpnt/TAS/aix4_1_4
   ```

   where `mntpnt` is the CD-ROM mount point.

3. Select **all_latest** as the SOFTWARE to install.
4. Click on **OK.**

3.4.2.2 Installation from the Command Line

Follow these steps to install TAS by the usual method:

1. Log in as **root.**
2. Place the CD in the drive.
3. Mount the CD-ROM using the following command, where `device` represents the path to the CD-ROM (for example, /dev/cd0), and `mntpnt` represents the directory mount point:

   ```
   mount -v cdrfs -oro device /mntpnt
   ```

4. To install the package, enter the following command at the system prompt, where `mntpnt` represents the mount point.

   ```
   installp 2>&1 -qacgNX -d /mntpnt/TAS/aix4_1_4 all
   ```

During the installation of TAS, the installation program adds the user and group *totalnet* to your system as the TAS administrative user and group, if it does not already exist.

3.5 Upgrading Earlier Versions of TAS

If you have a version of TAS and you want to upgrade to TAS 5.2, you need to run the `tnconvert` utility, which reads existing TAS configuration files, converts them, and saves them in the /etc/totalnet/convert directory. The `tnconvert` utility also prompts for and saves your new TAS 5.2 activation key. You need a new key to run `tnconvert`.

This process generates a log file in /etc/totalnet/convert/log.tnconv. When you complete installation, the post-installation script restores the configuration files saved by `tnconvert`, installs the new activation key, and installs and loads any required drivers. The `tnconvert` utility does not convert the administrative user and group names. You cannot use `tnconvert` to convert TAS 5.2 to an earlier version of TAS.

You can only make one-way conversions from earlier versions of TAS to TAS 5.2. Do a backup of TAS before upgrading.

Note

Make sure you have your **new activation key**. To request a new key, send e-mail to **tas52key@syntax.com** or mail or fax the key request form that comes with your TAS packaging.

3.5.1 Upgrading from TAS 5.x to TAS 5.2

Follow these steps to upgrade from TAS 5.x to TAS 5.2

1. Back up your current version of TAS, including all volumes.
2. Mount the TAS 5.2 CD-ROM.
3. Change directory to the location of `tnconvert` with the following command, where `mntpnt` represents the mount point of the CD-ROM device.

   ```
   cd /mntpnt/TAS/aix4_1_4
   ```

4. Enter the command `./tnconvert` and press **Enter**.

5. To verify, check the /etc/totalnet/convert/log.tnconv file.
6. Shut down TAS and TotalAdmin using the following commands:

   ```
   cd $TNHOME/usr/bin
   ./tnshut
   ./tas.sh stop totaladmin
   ```

7. Unload the drivers:

   ```
   ./tniunload
   ./atunload
   ```

8. If you use NetBEUI, also run the following command:

   ```
   ./nbuunload
   ```

9. Remove the old package using the following steps by typing:

   ```
   smit remove
   ```

10. Select **TAS softwares** and click on **OK**.
11. Install TAS 5.2 as described in Chapter 3.4.2, “Installation Steps” on page 19.
12. After a successful installation, run `tnvolck` to synchronize all volumes:

    ```
    cd $TNHOME/usr/bin
    ./tnvolck -a
    ```

13. Start the TotalNET system:

    ```
    cd TNHOME/usr/bin
    ./tnstart
    ```

3.5.2 Upgrading from TAS 4.1.1 to TAS 5.2

Follow these steps to upgrade from TAS 4.1.1:

1. Back up your current version of TAS, including all volumes.
2. Mount the TAS 5.2 CD-ROM in the drive.
3. Change directory to the location of `tnconvert` using the following command, where `mntpnt` represents the mount point.

   ```
   cd /mntpnt/TAS/aix4_1_4
   ```

4. Run `tnconvert`:

   ```
   ./tnconvert
   ```

5. To verify the success of `tnconvert`, check the /etc/totalnet/convert/log.tnconv file.

6. Shut down TAS and TotalAdmin using the following commands:

   ```
   cd /usr/tn
   ./tnshut
   cd totaladmin/W3/bin
   ./tnadmin.sh stop
   ```

7. Unload the drivers:

   ```
   cd /usr/tn
   ./tniunload
   ./atunload
   ```

8. If you have NetBEUI, run the following command:

   ```
   ./nbuunload
   ```

9. Remove the old package using SMIT, as follows:

   ```
   smit remove
   ```

10. Select the software and click on **OK**.
11. Install TAS 5.2 as described in Chapter 3.4.2, “Installation Steps” on page 19.
12. Run `atconvert`, where `dir` represents the directory path of your volumes:

    ```
    cd $TNHOME/usr/bin
    ./atconvert dir
    ```

13. Run `tnvolck` to synchronize all volumes in TAS.

    ```
    ./tnvolck -a
    ```

14. Start the TotalNET system:

    ```
    cd $TNHOME/usr/sbin
    ./tnstart
    ```

3.6 Connecting to TNAS

To access TNAS from your Web browser, you must have a browser that supports tables, forms, Java, and JavaScript. Supported Web browsers include Netscape Navigator 3.0 or higher and Microsoft Internet Explorer 3.0.1 or higher.

Follow these steps to connect to TNAS:

1. Using your Web browser, connect to TNAS by entering the URL below, where *hostname* is the host name of the AIX server on which TAS resides, and *nnnn* represents the TNAS port number, 7777 by default.

   http://hostname:nnnn

2. You will get the TotalNET Advanced Server V5.2 panel, as shown below:

Figure 11. TAS V5.2

3. Click on the center of the panel, or click on the **TNAS** icon**.**
4. At the TNAS log in panel, enter your **root** user ID and password to get the TNAS main panel, as shown below:

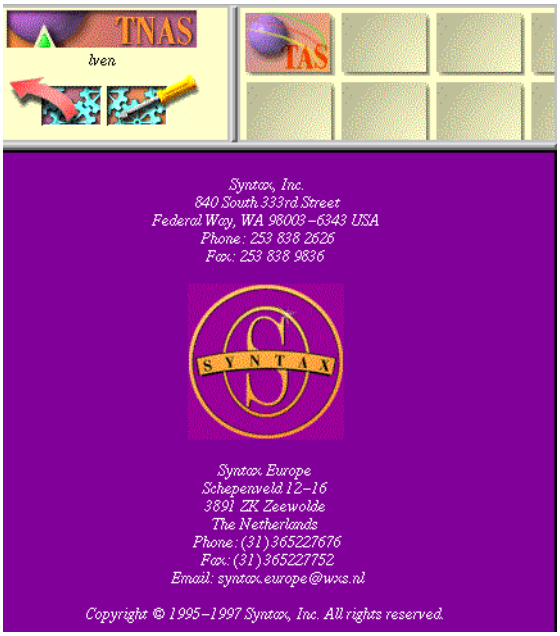


Figure 12. TNAS Main Panel

5. Click on the **TAS** icon, and you will get the TotalAdmin menu frame.

Figure 13. TotalAdmin Panel

6. At this point you must click **Initial Setup** to begin initial set up of TAS, as described in the next section.

Note

If you *upgraded* to TAS 5.2, you do not need to perform Initial Setup.

3.7 Initial Setup

The next step is to perform the Initial Setup configuration and complete all system-level configuration tasks.

Follow these steps to do the Initial Setup:

1. After you finish connecting to TNAS, click the first link in the TotalAdmin menu frame, **Initial Setup**, to get the following panel:

Figure 14. Initial Setup Panel

2. Click the **Start** button.
3. In the next panel, the TAS Activation Key window, you will have to enter the key license. Be aware that the key is case-sensitive. Then click **Next**.

Note

Without a license key, TAS supports only single-user mode. This can be used to evaluate TAS. Simply leave the Key field blank and click the **Next** button.

Figure 15. TAS Activation Key Panel

4. In the General TAS Settings panel, enter the values as requested.

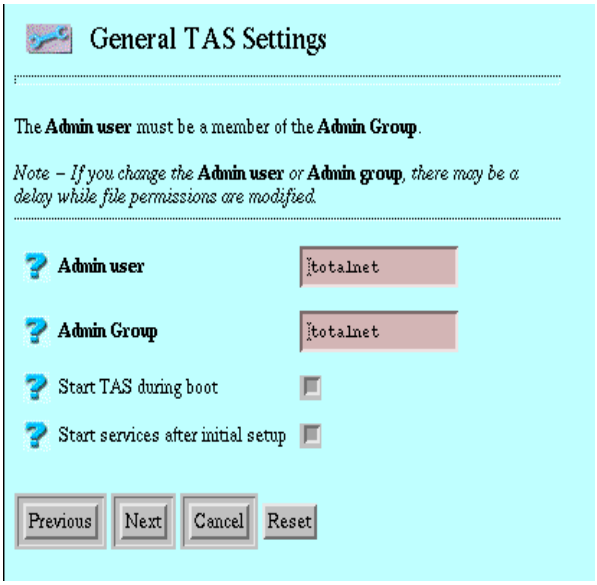


Figure 16. General TAS Settings Panel

If you select Start TAS during boot, TAS will be automatically started every time the AIX server is booted up. This is done by adding the following line in /etc/inittab:

```
tas:2:wait:/var/totalnet/usr/sbin/tas.sh start >/dev/console 2>&1
```

If you select Start services after initial setup, then TAS will start the default file service *hostname*, where hostname is the name of your TAS server hostname.

5. Use user *totalnet* and group *totalnet* as the primary administrative user of TAS. This user and group is automatically created during installation, as explained in Chapter 3.4, “TAS Installation” on page 17.
6. Click **Next**.
7. In the next panel, select **Enable LM-NT-OS/2 Compatibility** as your realm.
8. Click **Next**.
9. In the LM-NT-OS/2 Realm Configuration panel, enter your system hostname as the Server Name, and in the Workgroup field type in the

domain for your clients. Select **NetBIOS over TCP/IP** in the Transport List field.

If your clients support NetBEUI, you can also select NetBIOS over NetBEUI in Transport List, since it is supported by AIX. NetBEUI could be useful in a single LAN since it is a small and fast transport protocol. However, be aware that it works only within the subnet and cannot route data. If your system has multiple adapters, you must specify which device to use.

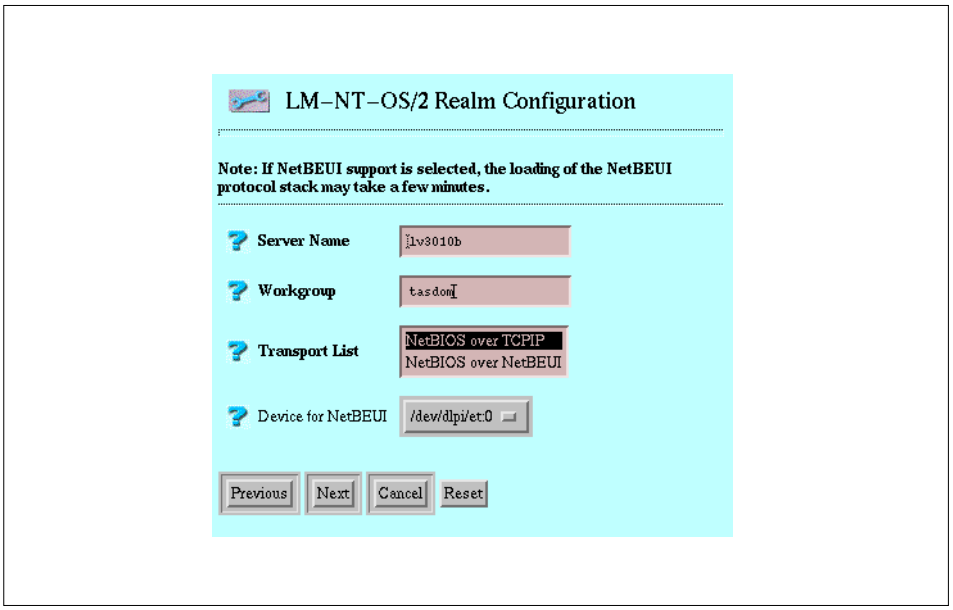


Figure 17. LM-NT-OS/2 Realm Configuration

10. Click **Next** until you get the **AppleTalk Compatibility Configuration**, and then click **Finish**.
11. You will get back to the **Initial Setup** panel containing the statement "Wizard successful."

Figure 18. Initial Setup Completed

3.8 General Administrative Tasks

In the following sections, we show you how to manage the processes and objects that provide file and print services to your clients. You must complete the steps in 3.7, “Initial Setup” on page 25 before you can perform any tasks described in this chapter.

Since you are already familiar with the menus displayed in the Initial Setup and connecting to TNAS, we will show you the links, rather than a complete menu-to-menu flow on how to perform the procedures.

As mentioned earlier, one of the greatest advantage of TAS is that there are no specific products to install and configure on the clients to be able to connect to the server and start sharing the resources already defined by TAS.

The following is an example of how to create a simple configuration. These steps should be followed in order:

1. Create a volume named VOL1 (covered in 3.8.9, “Administering Volumes” on page 36).
2. Create a printer DRAFT1 (covered in 3.8.10, “Administering Printers” on page 38).
3. Create a file service named FSRV1 with reference to volume VOL1 and printer DRAFT1 (covered in 3.9.4, “Creating and Modifying File Services” on page 42).

4. Connect from an NT client to a TAS server (covered in 3.9.10, “Connecting to TAS from an NT Client” on page 46).
5. Connect to the TAS printer service (covered in 3.9.11, “Configuring a TAS Printer from an NT Client” on page 50).

It is clear now that there is no separate printer service in TAS. This service is done by referencing the created printer to a file service.

Note

Please note that you do not have to complete all the sections listed below. You may jump to any section you need to perform, except for the five steps listed above, which must be done in order.

3.8.1 Starting TAS Services

TAS Services handles all other services in a TAS configuration. By default, TAS Services will start automatically after Initial Setup or system start up, unless you specify otherwise during Initial Setup.

Follow these steps to start the TAS system and set all services in all three realms to accept client connections:

1. Follow this link:

   System->System Administration->Start Services

   The Confirmation panel appears.
2. Click on **OK**.

   The Start all TAS Services panel appears.
3. Click on **OK**.

Now your TAS Services is enabled and automatically starts all services configured in the system.

3.8.2 Checking the TAS System Status

We recommend always checking your work after you complete it.

Follow these steps to check the status of services and client connections:

1. Follow this link:

   System->System Administration->Service Status

The Service Status panel appears. It will say either TAS system is enabled or TAS system is disabled.

2. When finished, click on **OK**.

3.8.3 Shutting Down TAS Services

Perform this step only if you need to, for instance, when making configuration changes, because all existing connections will be lost. Otherwise, go to 3.8.9, “Administering Volumes” on page 36.

You can specify the amount of time you want to elapse before shutdown. You may also enter a brief message to send to connected clients as shutdown nears and when shutdown commences. TAS will automatically send your message every five minutes until shutdown occurs.

Five minutes before shutdown, TAS sets all services to reject client connections.

You can cancel a pending shutdown.

Follow these steps to shut down the TAS system and set all services to reject client connections:

1. Follow this link:

   System->System Administration->Shutdown Services

   The System Shutdown panel appears.

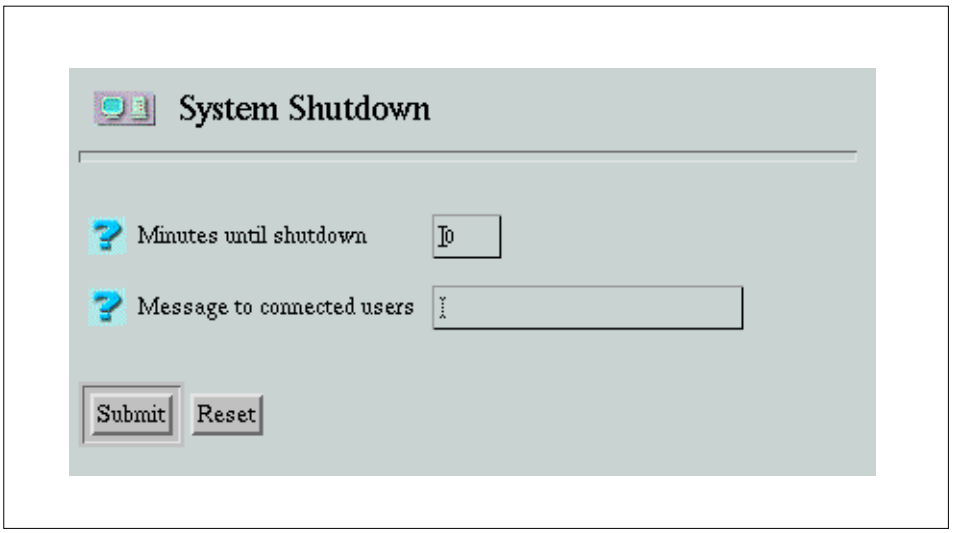


Figure 19. TAS System Shutdown Panel

2. Enter the values for Minutes until shutdown and Message to connected users.

   If you do not give any special message, clients will get a default message saying that the server is going down.

3. Click **Submit**.

   The Shutdown Services panel appears.

4. Click on **OK**.

3.8.4 Updating System Configuration

As a system administrator, you might want to change some parameters in your TAS configuration.

Follow these steps to change system configuration attributes:

1. Follow this link:

   System->System Administration->System Setup

   The System Setup panel appears as shown below.

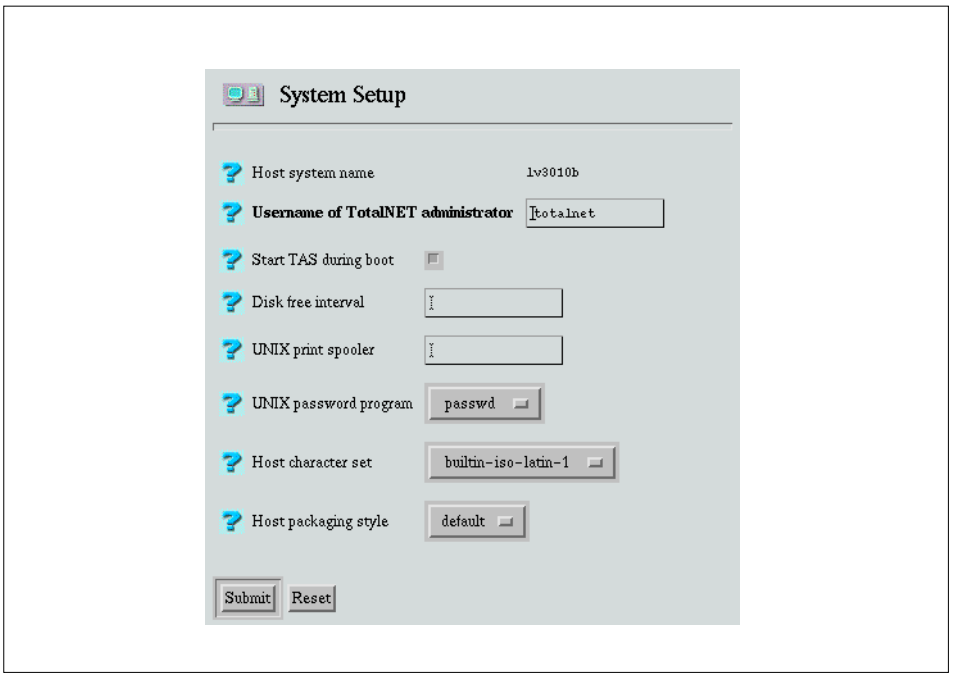


Figure 20. Updating System Configuration

2. Enter `totalnet` in the Username of TotalNET administrator field, and enter or select other values as needed.
3. Click **Submit**.

   The Updating System Setup panel appears.
4. Click on **OK**.

3.8.5 Accepting All TAS Services

TAS automatically sets its services to accept connections when started. If you need to set only a specific file service, please refer to 3.9.7, “Accepting Services” on page 45.

Follow these steps to make *all* defined TAS services accept client connections:

1. Follow this link:

   System->System Administration->Accept Service Connections

   The Confirmation panel appears.

2. Click on **OK**.

   The Accept Service Connections panel appears.

3. Click on **OK**.

   Your TAS system is now ready to accept new connections for all file services.

3.8.6 Rejecting All TAS Services

If you need to reject client connections from all services, you can follow the steps below. If it is only for a certain file service, please refer to 3.9.8, “Rejecting Services” on page 45.

Follow these steps to make *all* defined TAS services reject client connections:

1. Follow this link:

   System->System Administration->Reject Service Connections

   The Confirmation panel appears.

2. Click on **OK**.

   The Reject Service Connections panel appears.

3. Click on **OK**.

3.8.7 Listing Connected Users

Follow these steps to list TAS-connected users:

1. Follow this link:

   System->TAS Connected Users->User Information

   The Users panel appears.

2. Select from the list or enter in the text field the names of the users whose information you want to view.

3. Click **View**.

   The TAS Users information panel appears.

4. When finished, click on **OK**.

3.8.8 Disconnecting TAS Users

Follow these steps to disconnect selected users.

1. Follow this link:

   System->TAS Connected Users->Disconnect Users

The Disconnect Users panel appears.

2. Select or enter values for the attributes as needed.
3. Click **Submit**.

   The Disconnect Users panel appears.
4. Click on **OK**.

3.8.9 Administering Volumes

A TAS volume, which is just a directory path, resides in the AIX file systems. You can create volumes and assign user and group ownership and file protection masks. Users here are the users in the AIX server. File services can export *only* the AIX file systems *already defined* as a volume.

Follow these steps to create, modify, or delete a volume:

1. Follow this link:

   System->Volumes

   The Volumes panel appears.
2. You can enter the name of a new volume you want to add, or select from the list the volume you want to modify or delete.
3. Click **Create**, **Modify**, or **Delete**.

3.8.9.1 Creating A New Volume

If you click **Create**, the New Volume Definition panel will appear. Below is the top part of the panel in which you must enter the Volume name and Pathname:

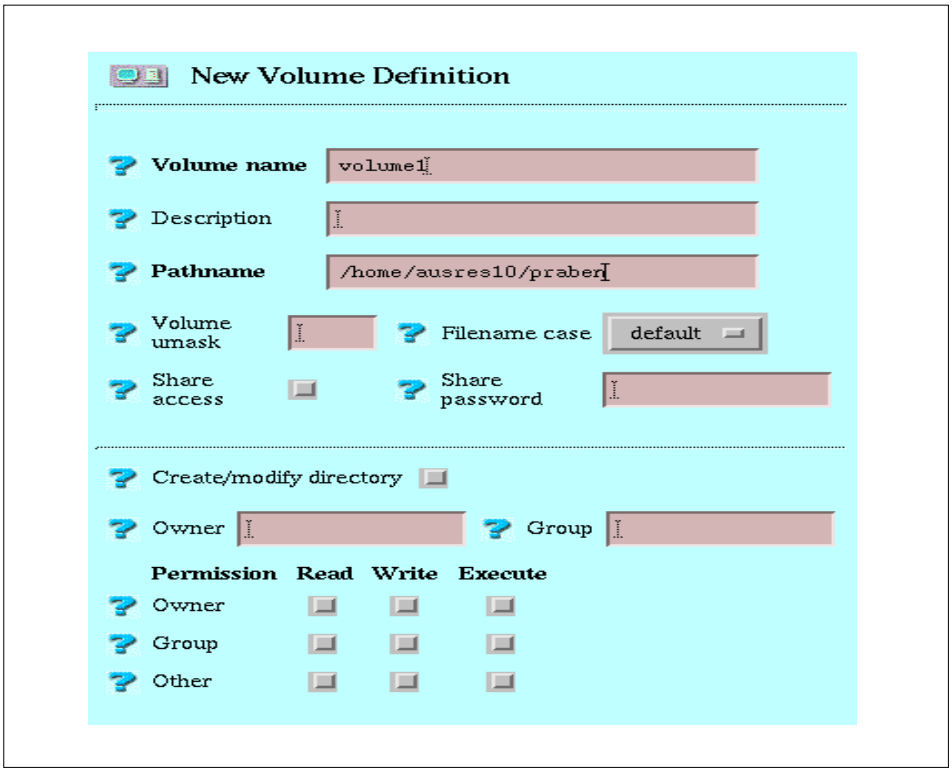


Figure 21. New Volume Definition

Volume name is the name used in `net use` and `map` commands.

Pathname is the full directory path beginning with a `/` (forward slash) as the virtual root of the volume.

You can have the share access option enabled by selecting the checkbox and providing a password. This way, your volume will be able to be shared by users. This option is available in the LM-NT-OS/2 realm only. If you select this option, TAS requires users to supply the share password to access the volume, so that it is accessible through share-level security mode service. Without this option, your volume will be accessed through the usual user-level security service.

There is an option to create/modify a directory if the directory you mention in the Pathname field does not exist in AIX. Please be aware that the parent directory must exist, because TAS only creates the lowest level of the directory path.

You also have the flexibility to determine the permission of the volume you create. To do so, perform the following steps:

1. Enter the **Volume name** and the **Pathname**.
2. Click **Submit**.
3. Click on **OK**.

3.8.9.2 Modifying A Volume

If you clicked **Modify**, the Update Volume Definition for *volumename* panel appears, which is the same as the New Volume Definition panel.

1. Modify as needed.
2. Click **Submit**.
3. Click on **OK**.

3.8.9.3 Deleting A Volume

If you clicked **Delete**, the Confirmation panel appears.

Click on **OK**.

3.8.10 Administering Printers

File services can export only those print queues defined as printers. The beauty of TAS is that you do not have to configure your queues to the TAS configuration.

What you need to do is:

- Choose which printers you need to define to the TAS configuration.
- To allow network clients access to a printer and its queue, define it by referencing it to LM-NT-OS/2 file services for the clients.

First in this section we show you how to add a printer to TAS, and then in 3.9.4, “Creating and Modifying File Services” on page 42, we reference it to our file service.

Follow these steps to create, modify, or delete a printer:

1. Follow this link:

   System->Printers

   The Printers panel appears. You can select the name of the printer you want to modify or delete, or type the name of a new printer you want to add.

2. In our example, we select DRAFT1 as the name of a printer we want to use.

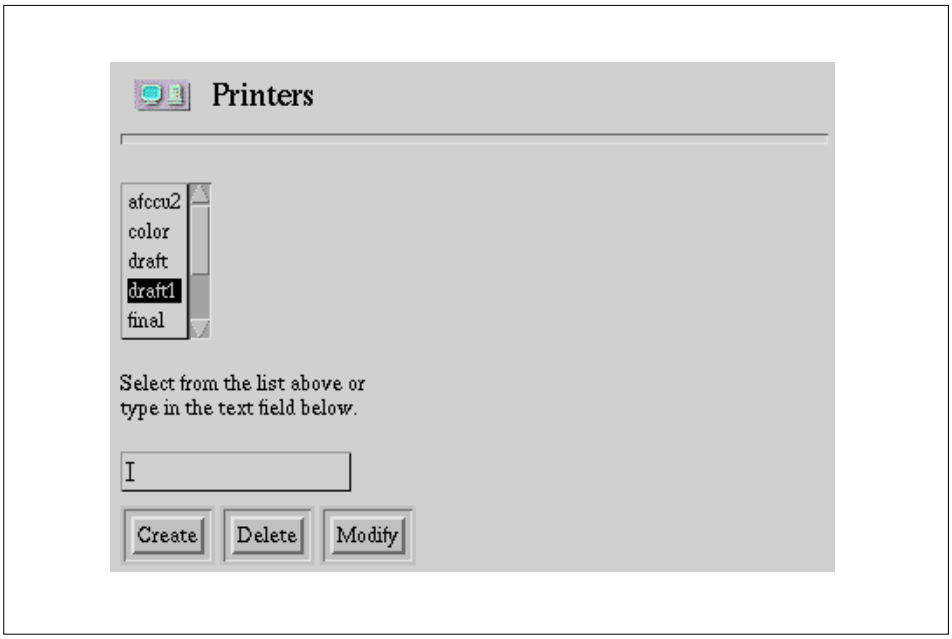


Figure 22. Add Printers Panel

3. Click **Create**, **Modify**, or **Delete**.

   In our example we click **Modify**.

   If after finishing Initial Setup you have more printers and queues added to your AIX system, you will need to define it to TAS configuration by clicking **Create**.

4. If you click **Create** or **Modify**, you will get the Printer Definition panel. Enter or select values as needed.

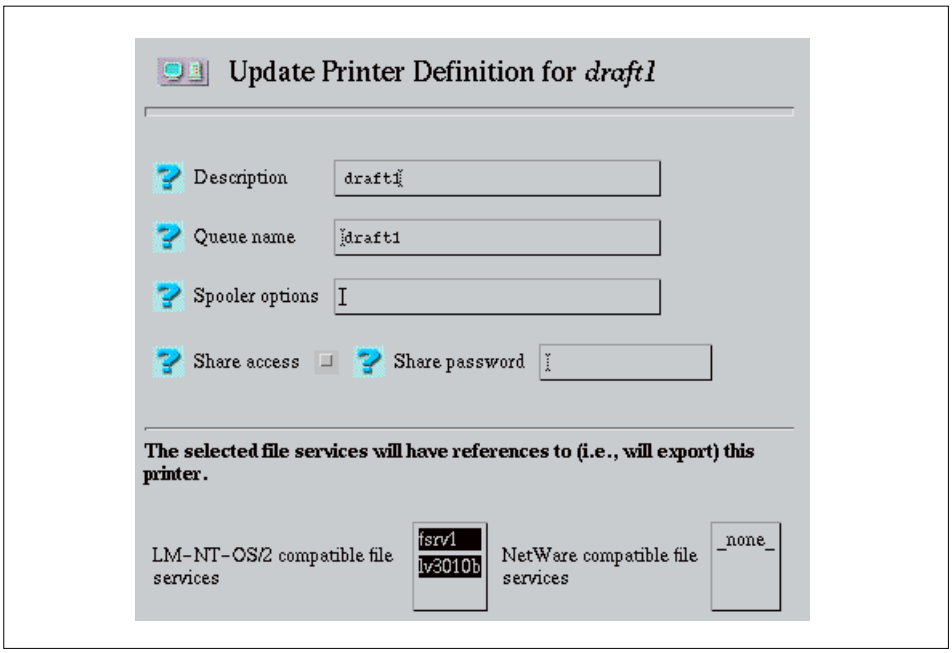


Figure 23. Update Printer Definition

Description - A printer description to appear in Network Neighborhood or at the `net view` command.

Queue name - The AIX print queue associated with the printer.

Spooler options - AIX command line options when a print job starts.

LM-NT-OS/2 compatible file services - Select the file services from which you wish to reference this printer.

Please note that you will only have your default file service on your panel, since you have not created one yet. You will have to reference this printer during file service creation to enable your clients to use it.

5. Click **Submit**, then click on **OK**.
6. If you click **Delete**, you get the Confirmation panel.
7. Click on **OK**.

Spooling is managed through the AIX system. TAS does not provide tools to manage your spool files.

3.9 Configuring Services

In this section we discuss the procedures for configuring and administering services in the LM-NT-OS/2 realm. As explained before, a client can access volumes and printers through a file service. We created a volume named VOL1 in 3.8.9, “Administering Volumes” on page 36, and defined a printer called DRAFT1 in 3.8.10, “Administering Printers” on page 38.

In this section we explain how to administer a file service to include our new volume and printer.

3.9.1 Starting LM-NT-OS/2 Services

Normally, your realm service is active now. By default, a realm service is activated automatically after Initial Setup, or at TAS system startup as discussed earlier in 3.8.1, “Starting TAS Services” on page 31. This capability gives you the option to start a specific realm, for instance in our case we want to start LM-NT-OS/2 service only.

Follow these steps to start the LM-NT-OS/2 realm and set its services to accept client connection requests:

1. Follow this link:

   LM-NT-OS/2 Realm->Configuration and Control->Start all LM-NT-OS/2 Services

   The Confirmation panel appears.

2. Click on **OK**.

   The Start all LM-NT-OS/2 Services panel appears.

3. Click on **OK**.

3.9.2 Checking Realm Status

As a system administrator, you will always make sure your job is done satisfactorily.

Follow these steps to check the status of the TAS system, transports, services, and client connections in the LM-NT-OS/2 realm:

1. Follow this link:

   LM-NT-OS/2 Realm->Configuration and Control->LM-NT-OS/2 Realm Status

   The LM-NT-OS/2 Realm Status panel appears:

When finished, click on **OK**. You now need to create a file service with reference to volume VOL1 and printer DRAFT1. Go to 3.9.4, “Creating and Modifying File Services” on page 42 now.

3.9.3 Shutting Down LM-NT-OS/2 Services

Follow these steps to shut down the LM-NT-OS/2 realm and set its services to reject client connection requests:

1. Follow this link:

   LM-NT-OS/2 Realm->Configuration and Control->Shutdown all LM-NT-OS/2 Services

   The Confirmation panel appears.

2. Click on **OK**.

   The Shutdown all LM-NT-OS/2 Services panel appears.

3. Click on **OK**.

3.9.4 Creating and Modifying File Services

Next, we will create a file service and we will call it FSRV1, as described in the following example.

Follow these steps to create or modify a file service in the LM-NT-OS/2 realm:

1. Follow this link:

   LM-NT-OS/2 Realm->Manage File Services

   The List of LM-NT-OS/2 File Services panel appears.

2. Select the file service you want to modify, or enter the name of a service you want to create in the text field. A file service name can contain up to 15 ASCII characters. It cannot contain spaces, and it must not begin with an asterisk. In our example we create FSRV1.

3. Click **Create** or **Administer**.

4. If you click **Create**, the New LM-NT-OS/2 File Service panel appears. Then go to step 7.

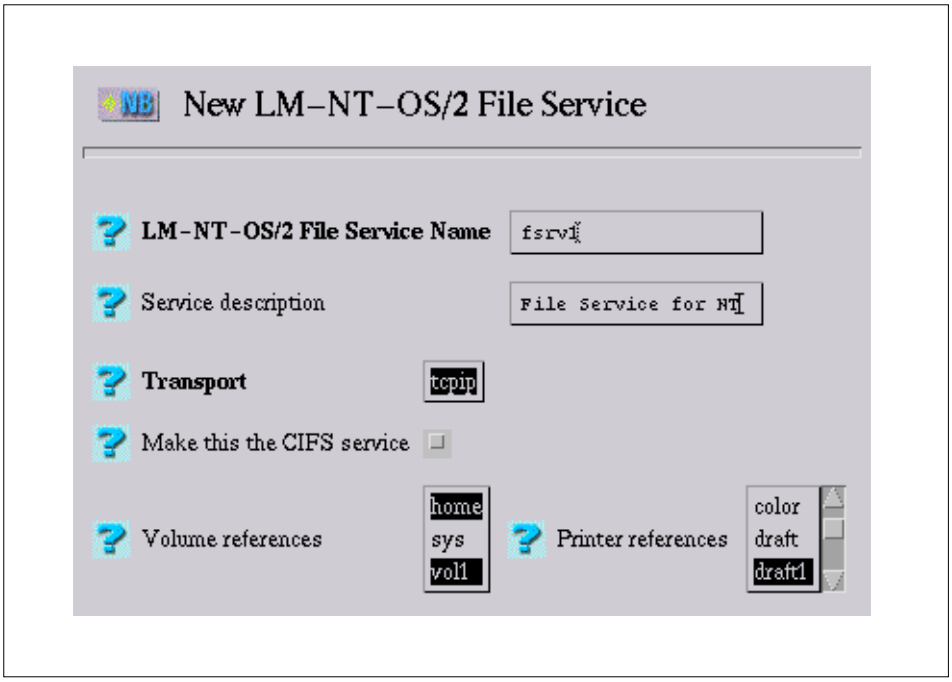


Figure 24. Creating a New File Service

In this example we select HOME, one of the default volumes created by TAS during installation, VOL1 which we just created, and DRAFT1 as the printer for this file service. You may select more than one volume or printer references for each file service you create. Be sure to start your new file service after you create it.

5. If you click **Administer**, the LM-NT-OS/2 File Service *servicename* panel appears.
6. Click **Configuration**, and the Update LM-NT-OS/2 File Service *servicename* panel appears.
7. Enter or select values as needed.
8. Click **Submit**.
9. Click on **OK**.

Now the file service is ready to be used by the clients.

3.9.5 Shutting Down File Services

When you shut down a file service, all connections will be lost. Clients currently connected will get a message: `server shutdown immediately`.

Follow these steps to shut down a file service:

1. Follow this link:

   LM-NT-OS/2 Realm->Manage File Services

   The List of LM-NT-OS/2 File Services panel appears.
2. Select the file service you want to shut down.
3. Click **Administer**.

   The LM-NT-OS/2 File Service *servicename* panel appears.
4. Click **Shutdown Service**.

   The Confirmation panel appears.
5. Click on **OK**.

   The Shutdown *servicename* Service in the LM-NT-OS/2 Realm panel appears.
6. Click on **OK**.

3.9.6 Deleting File Services

Before deleting a file service, it must be shut down.

Follow the steps below to delete a file service:

1. Follow this link:

   LM-NT-OS/2 Realm->Manage File Services
2. The List of LM-NT-OS/2 File Services panel appears.
3. Select the file services you want to delete.
4. Click **Delete**.

   The Confirmation panel appears.
5. Click on **OK**.

   The Delete LM-NT-OS/2 File Service panel appears.
6. Click on **OK**.

3.9.7 Accepting Services

LM-NT-OS/2 file service accepts client connection requests unless you set them to reject connection requests. Starting TAS also sets its services to accept connection requests.

Follow these steps to make your file service accept client connection requests:

1. Follow this link:

   LM-NT-OS/2 Realm->Configuration and Control->Accept Service Connections

   The Confirmation panel appears.

2. Click on **OK**.

   The **Accept all LM-NT-OS/2 Service Connections** panel appears.

3. Click on **OK**.

3.9.8 Rejecting Services

Follow these steps to make your file service reject client connection requests:

1. Follow this link:

   LM-NT-OS/2 Realm->Configuration and Control->Reject Service Connections

   The Confirmation panel appears.

2. Click on **OK**.

   The Reject all LM-NT-OS/2 Service Connections panel appears.

3. Click on **OK**.

3.9.9 Creating Terminal Services

TAS does support terminal service. This means you can use your favorite terminal emulator program to open a session. You need a terminal emulator that supports NetBIOS, such as Kermit.

There are two operating modes: online and local. You start online mode from the Windows prompt by typing the command you need for your terminal emulator program, and the local mode by pressing **Alt-Z** to open a session.

From a local mode you can open another session, quit from current session, or do a shell command.

Follow these steps to create a terminal service:

1. Follow this link:

   LM-NT-OS/2 Realm->Manage Terminal Services

   The List of LM-NT-OS/2 Terminal Service panel appears.
2. Enter the name of a service you want to create in the text field.
3. Click **Create**.
4. Enter or select values as needed.
5. Click **Submit**.
6. Click on **OK**.

For other services, please refer to the *TAS Administration Manual*.

3.9.10 Connecting to TAS from an NT Client

After starting your LM-NT-OS/2 realm on your TAS server, you will be able to see the Workgroup from NT. Follow these steps:

1. From the Windows NT desktop, select the **Network Neighborhood** icon. The following is part of the Windows NT desktop:

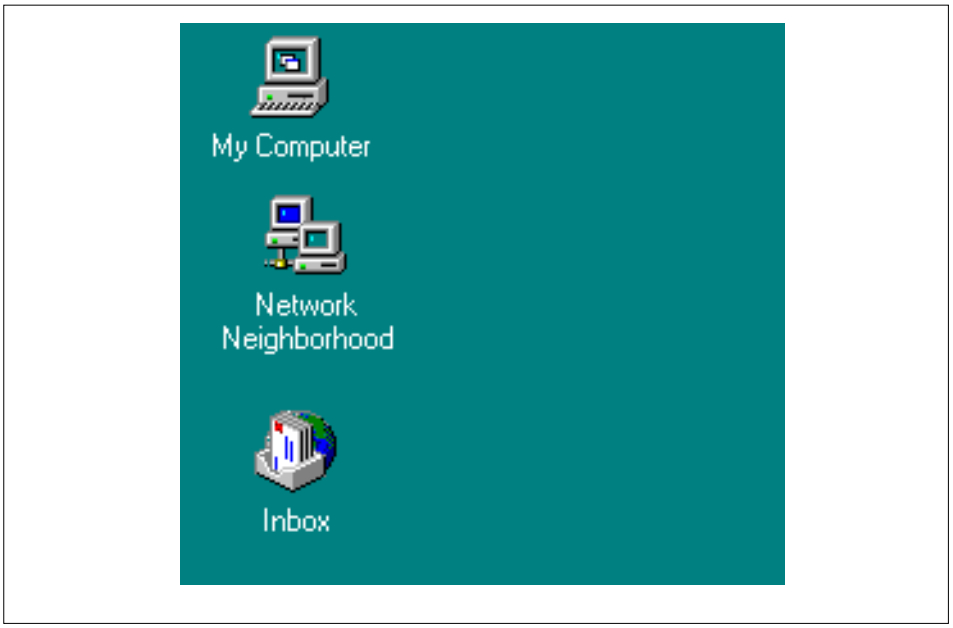


Figure 25. Windows NT Desktop

2. From the Network Neighborhood panel, select **Entire Network**.

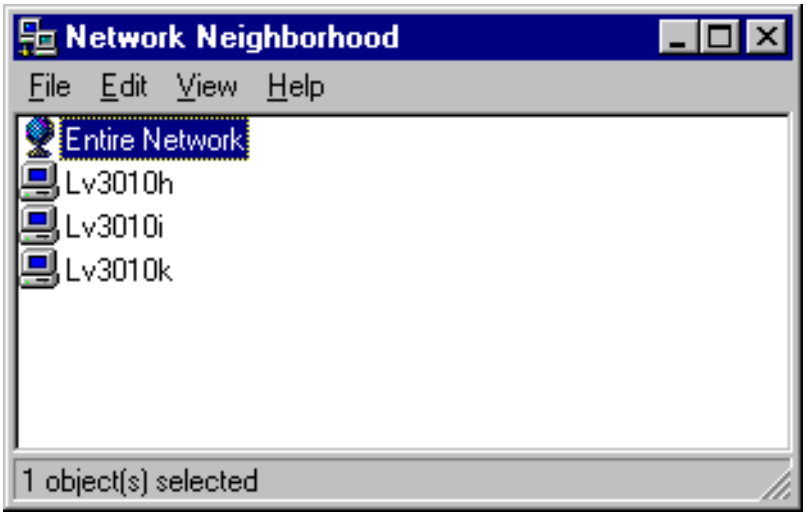


Figure 26. Network Neighborhood Window

You will get the Entire Network window.

3. Then select **Microsoft Windows Network**.
4. You will get a window similar to the following:

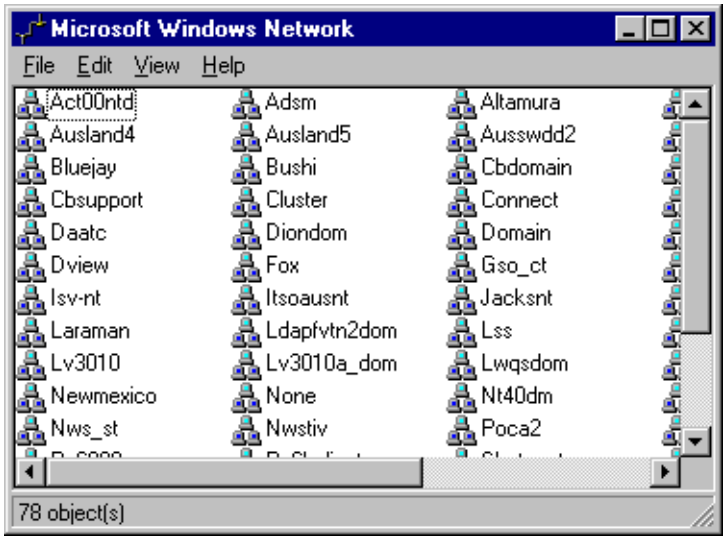


Figure 27. Displaying Entire Network

We will find our workgroup, Workgroup, is there. By double-clicking it, we get our file services that were previously defined. For instance, when we select FSRV1, we will get the following panel:

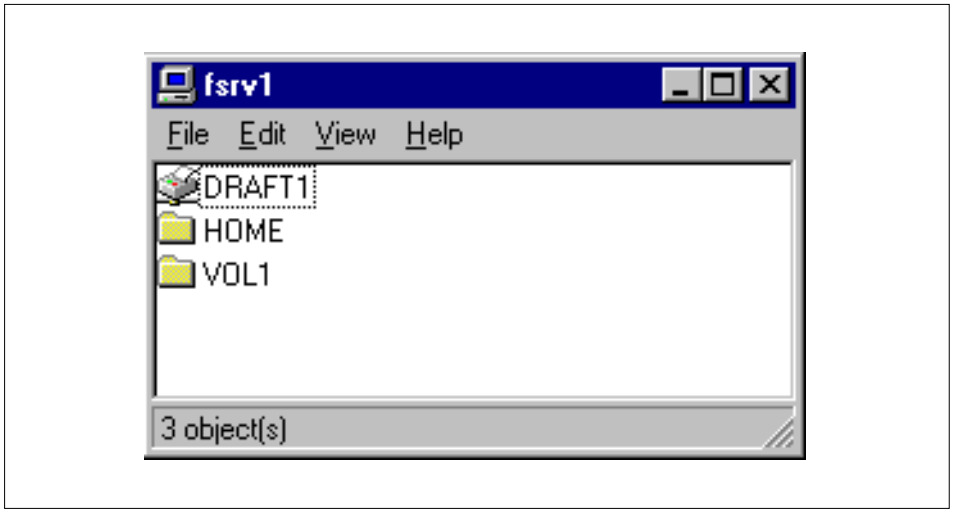


Figure 28. Accessing a File Service from an NT Client

We see our printer, DRAFT1, and our two volumes, HOME and VOL1, are there.

5. By selecting VOL1, we enter that directory and get the following panel which is the content of directory /home/ausres10/ben in the AIX server.

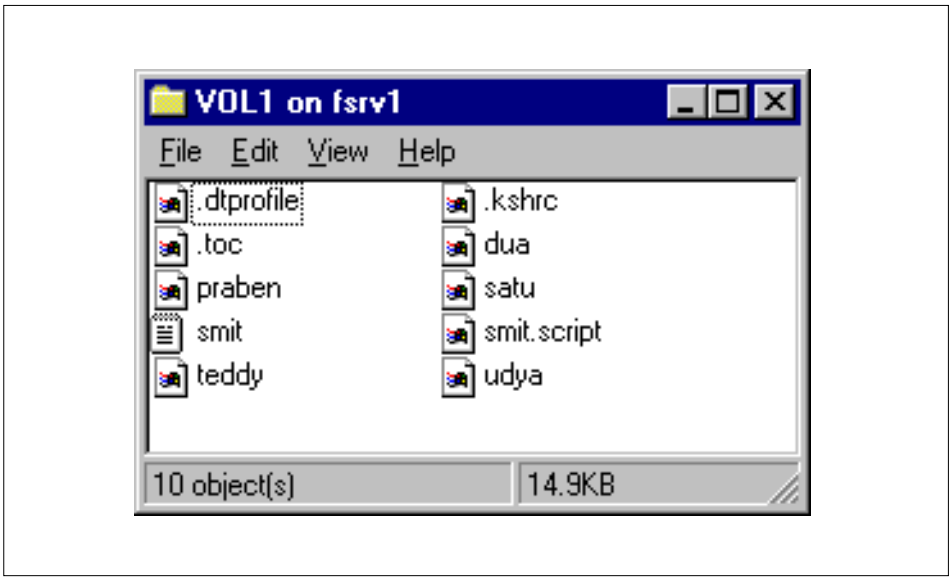


Figure 29. Accessing a Volume

The system administrator can now modify the application so that these processes are done automatically, without the end user's involvement.

3.9.11 Configuring a TAS Printer from an NT Client

Your AIX printers are now available to NT clients. The only thing left to be done on your client is perhaps installing the correct driver for the printer type you use, if it is not yet installed on your PC. You will be asked to install it, and you have the choice to install it on your NT client.

If you double-click on the **DRAFT** icon, you will get the following window:

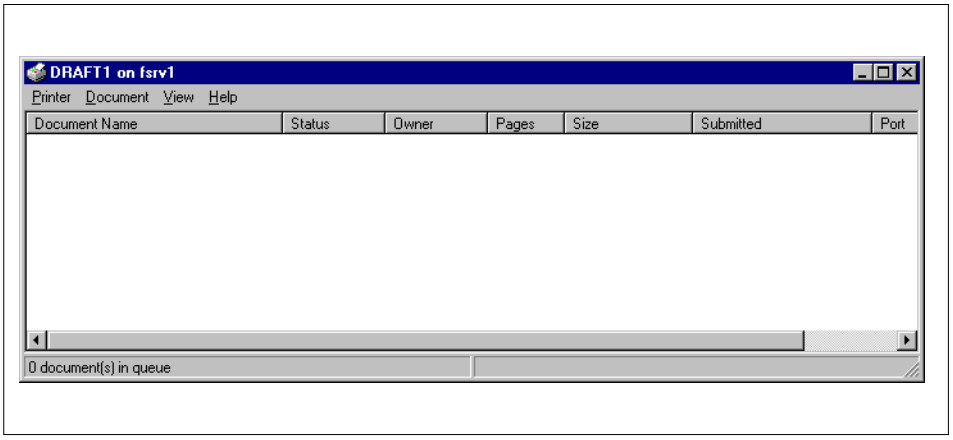


Figure 30. Displaying Printer DRAFT1 from an NT Client

Your printer is now ready to be used by your clients.

3.9.12 Miscellaneous

In AIX, you can have files with the same name but in a different case, for instance file1 and File1. TAS has the ability to rename these files so that it will be different from the NT client's point of view.

3.10 Security

In any environment, especially a client/server environment, security is always an important issue. Our security concerns might be for resources we have on the disk, or passwords passing across the network.

3.10.1 Resources

TAS provides security for accessing resources, just like in AIX. From the File Service and Volume creation panel discussed earlier, you can see that you can specify the permission for any resource you create.

For example, during a creation of a volume (see Figure 21 on page 37), we have the following parameters:

Volume umask - Permission for files created on the volume.

Permission - AIX file permission to read, write, and execute.

The parameters above are exactly like standard AIX parameters you are familiar with.

With the LM-NT-OS/2 realm, you can also specify share access mode. If you select this option you have to provide a share password, used to access the volume.

You can also modify AIX file attributes under a volume using the following steps:

1. Click the **File Permission** link, and the following panel appears:

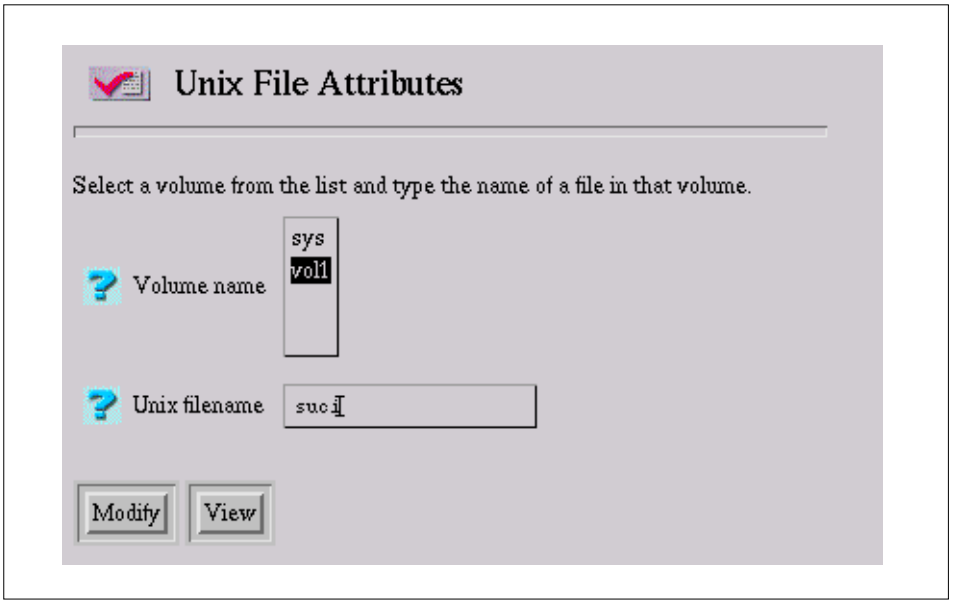


Figure 31. Selecting Volume and Filename to Change

2. Select or enter values as needed.
3. Click **Modify** to get the following panel:

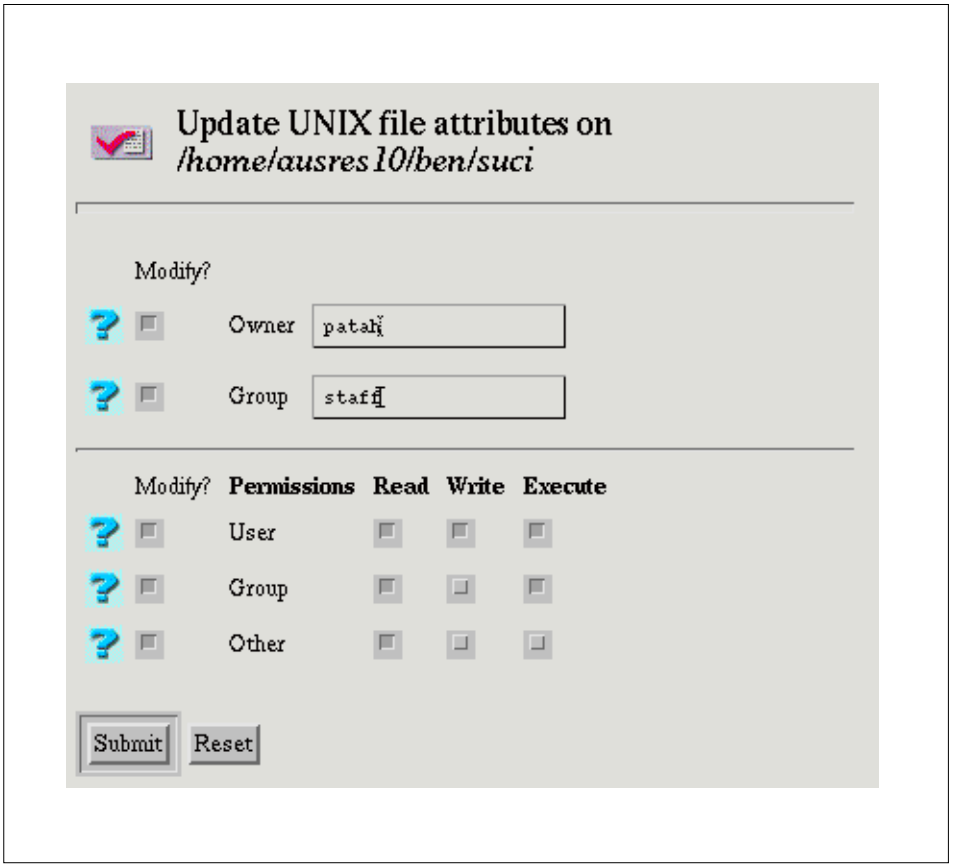


Figure 32. Updating File Attributes

4. Click **Submit**.
5. Click on **OK**.

3.10.2 Secure Authentication

To be able to access files and resources, all clients must have file service authentication. TAS provides two methods for authenticating clients: AIX authentication and secure authentication.

By using AIX authentication, users send passwords in text-mode over the network. The file service program in TAS checks these passwords using a standard AIX procedure such as /etc/passwd or NIS.

Secure authentication requires a separate, TAS-maintained database. A client using this method does not send text passwords over the network. Instead, the client and server exchange a random message, and each encodes it with the user's password. The client sends the result of its encoding to the server, and the server compares it with the result of the server's encoding.

Follow these steps to create, modify, or delete a secure authentication user:

1. Click the **Passwords** link.

   The Password Users panel appears.

2. Enter the name of the user you want to add in the text field.
3. Click **Create**, and the Specify New Passwords panel appears.

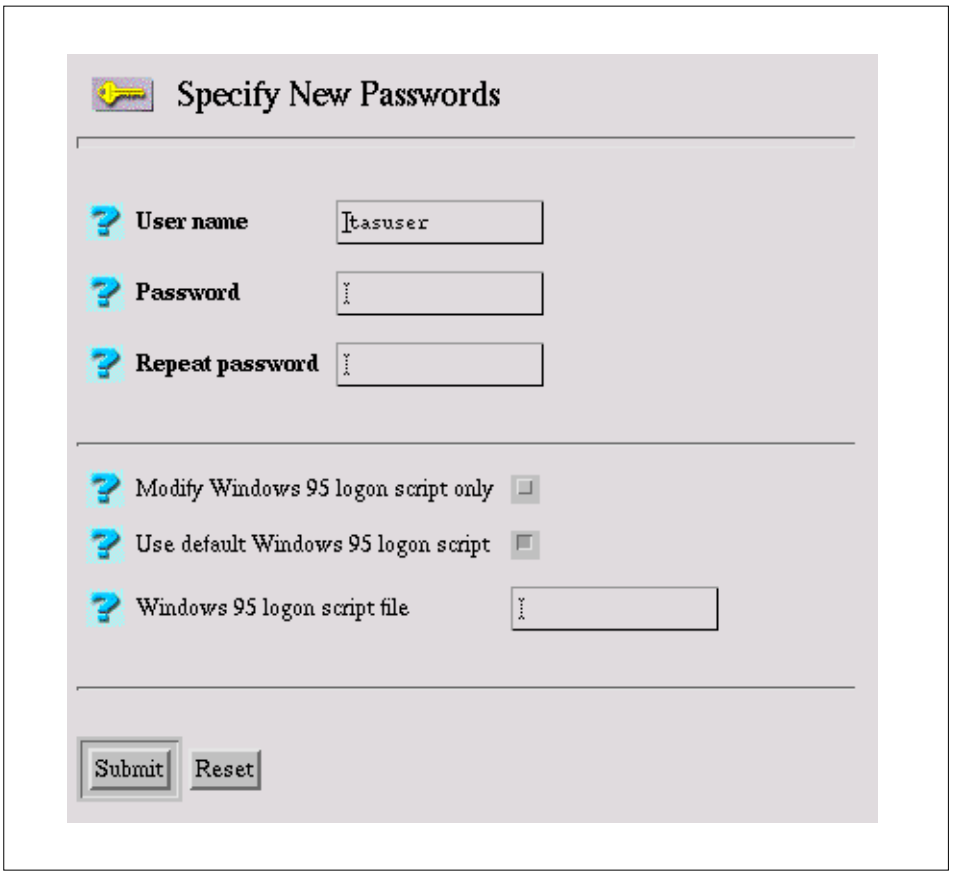


Figure 33. Specify Secure Authentication Password

Enter values as needed. Be sure that the user name you put in User name field is an existing user in AIX.

4. Click **Submit**.
5. The Creating new Passwords for *username* panel appears.
6. Click on **OK**.

   The user *tasuser* is now TAS secure-authenticated.

3.10.3 Configuring LM-NT-OS/2 File Authentication

We also have the facility to configure security on a realm basis. This means that the file service we create will be protected by the realm, and access by the clients will be verified either by local authentication, proxy server

authentication, or share mode. We will discuss all of these options in the following section.

Follow these steps to configure LM-NT-OS/2 file authentication:

1. Follow this link:

   LM-NT-OS/2 realm->Manage File Services

2. Select the file service you want to configure.
3. Click **Authentication and Service Mode Options**.

   The Authentication Mode panel appears:

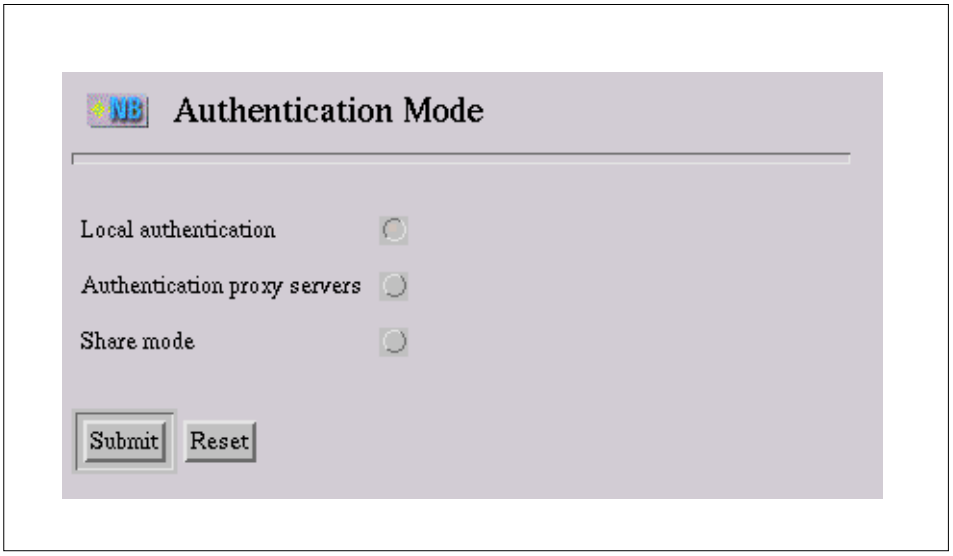


Figure 34. Changing the Authentication Mode

4. You now have the options to choose Local authentication, Authentication proxy servers, or Share mode.

3.10.3.1 Local Authentication

This means the authentication is done by a file server in the LM-NT-OS/2 realm. If the server cannot verify a client's user ID and password, it refuses the connection. If the realm uses local authentication, it does not consult a proxy server. You may choose open authentication or secure authentication. With open authentication, the client and server exchange text passwords. With secure authentication, the client and server exchange a series of

messages that allows the server to verify that the client knows the correct password, without transmitting the password.

3.10.3.2 Authentication Proxy Servers

This means the authentication is done by another server. If the other proxy server cannot verify a client's user ID and password, it refuses the connection. If it accepts the connection, then the local server looks up the user name using /etc/passwd or NIS.

3.10.3.3 Share Mode

If you selected Share mode, it means the user of the service can share the files created by the clients.

3.11 Year 2000 Compliance

TAS adheres to the computer industry's guidelines for compliance with Year 2000 standards. There are several client/server protocols such as Server Message Block Protocol (SMB), NetWare Core Protocol (NCP), and Apple File and Print Protocol (AFP), and TAS supports all of these protocols with respect to Year 2000 conformance. All TAS programs correctly process leap years, and conform with Option One of the *Y2000 Developer's Guide*, making them Year 2000-compliant.

3.12 General Issues

The following are some general issues you may find in your installation. For up-to-date information about issues with TAS 5.2, access the following Syntax URL:

`http://www.syntax.com/support/guest/docs/tedoc.htm`

Passwords

The `tnpasswd` utility changes the TAS-encrypted password before attempting to change the AIX password. If it fails to change the AIX password, you cannot use the `tnpasswd` command to resynchronize passwords. To synchronize TAS and AIX passwords, change the AIX password using SMIT and provide it with the same password you use to change the TAS password.

Windows Clients

If your network includes Windows NT and Windows 95 clients, set the *Use Client Specified File Time Stamps* attribute to `on` for all LM-NT-OS/2 file

services you create. This setting enables icons for connected file services to display correctly.

Documentation

For slower-loading browsers, HTML documentation text may appear garbled. Click your browser's **Refresh** or **Reload** button to correct this. If you use Internet Explorer 3.0, some links may not work, and you may need to click **Refresh** or **Reload** to load an entire document.

"case-preserving-link" Attribute

The *case-preserving-link* attribute of TAS 5.0 and 5.1 no longer exists in TAS 5.2. If you had it set to on, `tnconvert` ignores the value in the old configuration and sets the value to `preserve` in the new configuration.

"no-login" Attribute

TAS 5.2 does not support the *no-login* attribute for file services. The `tnconvert` command replaces it using the *login-control* attribute in the new configuration. This way, the form *no-login <list of user names>* changes to *login-control deny <list of user names>*.

3.13 Troubleshooting

TAS installation and basic configuration is generally quite simple. For a more complex environment, however, you may encounter some problems, and in this section we give you information on some common problems you might have in TAS configuration.

3.13.1 Customer Service Request

Usually when you contact Syntax Technical Support, you will be asked to provide a CSR or Customer Service Request report. This is used to verify your host system configuration, licensing, server activity logs, configuration attributes, connection statistics, and problem-solving diagnostics.

Follow this link to generate a CSR:

System->Generate Support Info

You can now e-mail the output to `support@syntax.com`.

If you like, you could generate a CSR report from command line using the `csr.tn` command as follows:

```
/var/totalnet/usr/bin/csr.tn > csr.txt
```

where `csr.txt` is the output file.

Before contacting Syntax, please ensure that you have the following information:

- The Syntax AAA serial number listed on your media
- The version of TAS you are using
- The version of your AIX you are using
- The type and model of your machine
- Circumstances leading to the problem
- Any error messages displayed or logged

3.13.2 Some Hints and Tips

The following are some problems we encountered. For a complete troubleshooting guide, please refer to the TAS System Administration Manual.

Initial Setup Wizard does not work

During installation, it is possible that the installation process somehow does not work as expected in configuring the TAS browser programs, and causes Initial Setup to fail. Please run the Initial Setup Wizard from the command line using the `/var/totalnet/usr/sbin/tnsetup` command. One of the most common causes is that you have installed and removed an older TAS version from your system before doing this Initial Setup program.

Fail to connect to http://hostname:7777

This usually happens if you have TAS components in your system before installing TAS. This causes the TNAS port number to not set to the default, which is 7777. Please check your smit.log file or $TNHOME/tassetup.log file and verify this. It is likely that your TNAS port number is 7778.

You cannot start TAS

Check that your AIX NetBIOS is not running. Running NetBIOS components from other sources may cause problems.

Client cannot connect to file services

In this case, your client receives the message, `network problem occurred`, when trying to access a file service. Check that you have the correct license

ley. The most-probable cause is the number of users is exceeded. You can verify this by checking the log through:

LM-NT-OS/2 Realm->View LM-NT-OS/2 Log File

You will find an error message: `number of users exceeded`.

Client cannot display the TAS workgroup

You should modify your file service and look for the Browse master option. Change it to on (the default is off). You also can change the Browse election bias to 32 for Windows NT servers (the default is 0).

Client cannot access the TAS server

It is possible that your clients cannot detect your file services for no apparent reason, and without error messages. This is probably because the NetBIOS daemon is not running. Use the `ps -ef` command the check that the NBname and NBdaemon processes are running. Another possibility is those NetBIOS daemons are still active, even though the TAS server has been shut down. Terminate them using the `kill` command, and then restart the TAS server.

Disconnected clients still appear connected

There are two causes of this problem.

- TAS is waiting for the timeout period to elapse before terminating the appropriate process, which is five minutes. Configure TAS to use a keepalive program through:

  LM-NT-OS/2 Realm->Manage File Service->servicename-> Administer-> Configuration

  Then activate keepalive. You can specify the number of minutes for TAS to terminate a dead process, the default is one minute. Using keepalive, TAS checks the status of its clients every minute, and terminates the service if there is a dead process.

- Another possibility is TAS is unable to terminate the process in an orderly fashion. You will need to restart TAS if you really need this dead process to disappear.

Chapter 4. AIX Connections

In this chapter we discuss the connection setup between Windows NT and AIX using AIX Connections.

We will also discuss how AIX Connections works in providing services such as file or printer service to Windows NT clients. In our examples we use AIX 4.3 with AIX Connections 4.1.6 and Windows NT 4.

4.1 AIX Connections Overview

AIX Connections is software installed in AIX to provide services such as file service and printer service to clients. Since Windows NT is widely used, it is necessary for us to know how to implement AIX Connections in a client/server environment where Windows NT is present.

As of the writing of this redbook, AIX Connections 4.1.6 is the most current version of the product since its announcement in 1995. This software is based on TotalNET Advanced Server, or TAS, from Syntax, Inc., which we discuss in Chapter 3. In this new version there are *realms*, which are basically sets of software that provide services to different types of clients. There are three realms:

- NW Realm for Novell NetWare clients
- NB Realm for NetBIOS clients
- AT Realm for Macintosh clients

NT machines usually use NetBIOS over TCP (RFC 1001/1002) as a communication protocol, even if a customer chooses different protocols like NetBEUI or NWLink (IPX/SPX-compatible protocols) that are shipped with the NT operating system. However, since NetBIOS is the most common protocol in NT machines, we use it in our description. To give services to Windows NT clients we need to have NB Realm installed. Since this is already a part of AIX Connections, we do not need to purchase it separately. The **NB Realm** corresponds to the **LSserver** component of earlier releases of AIX Connections.

There is not much difference, conceptually, between AIX Connections and TAS, which we discuss in “TotalNET Advanced Server” on page 13. Therefore, we focus on the steps you must take to perform the tasks.

4.2 System Requirements

The following sections describe the system requirements for creating a connection between Windows NT and AIX, using AIX Connections.

4.2.1 Server Hardware Requirements

AIX Connections runs on any machine that supports the AIX operating systems, except for diskless or dataless machines. You will need to have Ethernet, a token-ring, or an FDDI adapter installed on your server.

FDDI is only supported by NetBIOS over TCP (RFC 1001/1002) and IPX/SPX. No support to FDDI is provided by NetBEUI or AppleTalk Protocol.

AIX Connections does support ATM in LAN emulation.

4.2.2 Server Software Requirements

The following software must be installed on your server to run the current version of AIX Connections:

- AIX 4.1.5 or later
- NetBIOS 2.1.4 or higher
- Web browser with forms support (for example, Netscape 2.0 or higher) if you plan to use the Web-based AIX Connections Admin tool
- License Use Management client software

4.2.3 Client Hardware Requirements

All clients must have a LAN adapter installed.

4.2.4 Client Software Requirements

To use AIX Connections, all clients must have a LAN requester, such as:

- IBM’s LAN Server Version 3.0 or higher
- Microsoft’s LAN Manager
- Microsoft’s Windows for Workgroups
- Microsoft NT

In our case we have Microsoft NT installed on our clients.

4.3 AIX Connections Installation

The AIX Connections product is put into an installation bundle, which is called **connect.Bnd**. By selecting this, you will install all necessary software.

During installation, AIX Connections will automatically configure some basic configuration in NetBIOS Realm. It creates:

- A file service
- A terminal service
- A volume reference to the home and pccode volumes

The installation process also edits the /etc/inittab file to automatically start realms during reboot, by adding the following lines:

```
rcnwserver:2:wait:/etc/rc.nwserver start > /dev/null 2>& # start NWserver
rcmacserver:2:wait:/etc/rc.macserver start> /dev/null 2>&1 # start MACserver
rclsserver:2:wait:/etc/rc.lsserver start> /dev/null 2>&1 # start LSserver
```

For this purpose, a set of rc files is created in the /etc directory:

- rc.lsserver
- rc.nwserver
- rc.macserver

The file /etc/rc.lsserver is what we need for our environment.

AIX Connections will also automatically configure the /etc/dlpi.conf file for you. It will edit the lines relative to the LAN adapter you have installed on your machine. For instance, if you have a token-ring adapter, the following line will be edited (removing the comment):

```
d+      dlpi    tr,r /dev/dlpi/tr    # streams dlpi token ring driver
```

Notes

Please be sure that NetBIOS is already available in your system. If NetBIOS is not yet installed, please install it now before proceeding to the next step.

Log in as root, and then from command line enter:

```
smit install_latest
```

Select your input device, for instance /dev/cd0, then click on **OK**.

Select **connect.Bnd** as SOFTWARE to install and click on **OK**.

Installing AIX Connections without PostScript documentation will require about 25 MB of disk space.

Notes

Please be sure to configure TCP/IP first and have your hostname set. AIX Connections will use the hostname of your workstation to set up service names for you.

4.4 AIX Connections Configuration

Configuring AIX Connections can be done in two ways, using the SMIT menu or using the Web-based tool. We will have to configure the realm we need, NB Realm, NW Realm, or AT Realm. In our configuration we need NB Realm, which is for NetBIOS.

4.4.1 Quick Start

AIX Connections provides an easy tool called Quick Start. It will set the basic configuration for any of the three realms, then starts the configured services on your system. You can only use the Quick Start tool before any other configuration has been done, since it may cause unpredictable results. Do not use the Quick Start tool if you have migrated to the current version.

To run Quick Start, do the following steps:

- Type `smit`
- Select **Applications**
- Select **AIX Connections**

You will get the following SMIT menu:

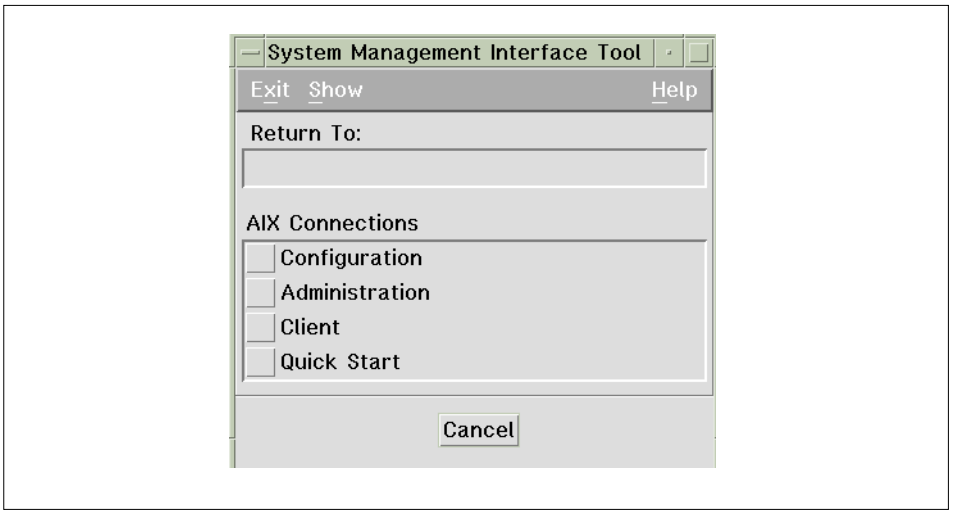


Figure 35. AIX Connections Main Menu

This is the AIX Connections main menu which you can also access by using the SMIT fastpath: `smit aconn`. From now on we will use this AIX Connections main menu as our starting place when in configuring AIX Connections.

1. Select **Quick Start** from the above menu.
2. Select **NB** as the realm.
3. Select **RFC** as your protocol.
4. Select the device, in our case it is `tr0`.
5. Click on **OK**.

At this point the configuration is complete. If you have more than one interface, you can repeat the steps above to configure another service for this interface.

4.4.2 Checking the Result

Your NB Realm server is now up and running with two default volumes created, home and pccode. NetBIOS is also active with one LANA configured and started.

A good system administrator always checks the result of their tasks.

To check that your volumes have been created, select the following path:

AIX Connections Main Menu->Configuration->Volumes->List of Defined Volumes

To check that the NB Realm is running, select the following path:

AIX Connections Main Menu->Administration->Server Status

If you are satisfied with the current default configuration, you can go to 4.4.5, “Post-Configuration Tasks” on page 77. Otherwise, if you want to do additional configuration now, continue to 4.4.3, “Additional Configuration” on page 66.

4.4.3 Additional Configuration

In this section we discuss the steps you need to take to perform additional configuration to your system. Again, we always start from the AIX Connections main menu which you can access by typing `smit aconn` from your command line.

4.4.3.1 Changing AIX Connections System Name

Follow these steps to change the AIX Connections System Name:

1. Select **Configuration** from the AIX Connections main menu.
2. Select **System Name**.
3. Type a new name for your system.
4. Click on **OK**.

We recommend that your system name is the same as your hostname. Also if you do not set a system name, Quick Start will automatically set the system name to be the first service name entered.

4.4.3.2 Changing the Workgroup

By default, AIX Connections server belongs to the WORKGROUP workgroup. This mean that when you browse the network and double-click on the workgroup named WORKGROUP, a window pops-up containing all the machines belonging to that workgroup, included the AIX Connections server. To change it, follow these steps:

1. Select **Configuration** from AIX Connections main menu.
2. Select **Realms**.
3. Select **Modify Realm**.
4. Select **NB**.

5. Fill-in the **Domain Name**, indicating the name of the workgroup to which you want your server to belong.
6. Restart the server.

4.4.3.3 Creating/Adding Interfaces

You may have a need to add more interfaces to include in your configuration.

Before adding a new interface, you must define a new LANA which the interface refers to. In order to create a new LANA follow these steps:

1. Select:

   Configuration -> **NetBIOS** -> **LANAs** -> **Add LANA Configuration**
2. Chose the Protocol (usually **RFC 1001/1002** for NT machines)
3. Fill the **RFC 1001/1002** dialog box. Usually the only parameter you must modify is the **TCP/IP Interface**, to match the physical interface you want to link. For a further explanation of the meaning of the other parameters, refer to the help on line.
4. Press Enter when finished

When finished you can add an interface, following these steps:

1. Follow this link:

   Interfaces->Manage Interfaces->*select a realm*

   In our case we select NB Realm.
2. Assign your interface an appropriate name. By appropriate we mean it starts with en for Standard ethernet, et for IEEE 802.3, or tr for Token Ring.

   You will have the AIX Connections Interfaces panel.
3. Choose the device name, /dev/lana<x>

   where <x> is the LANA Number.
4. Click on **OK**.

4.4.3.4 Creating/Adding Volumes

Follow these steps to add volumes:

1. Follow this link:

   Volumes->Manage Volumes
2. Enter the volume name in the Volume Name field.
3. Click on **OK**.

You will get the following screen:

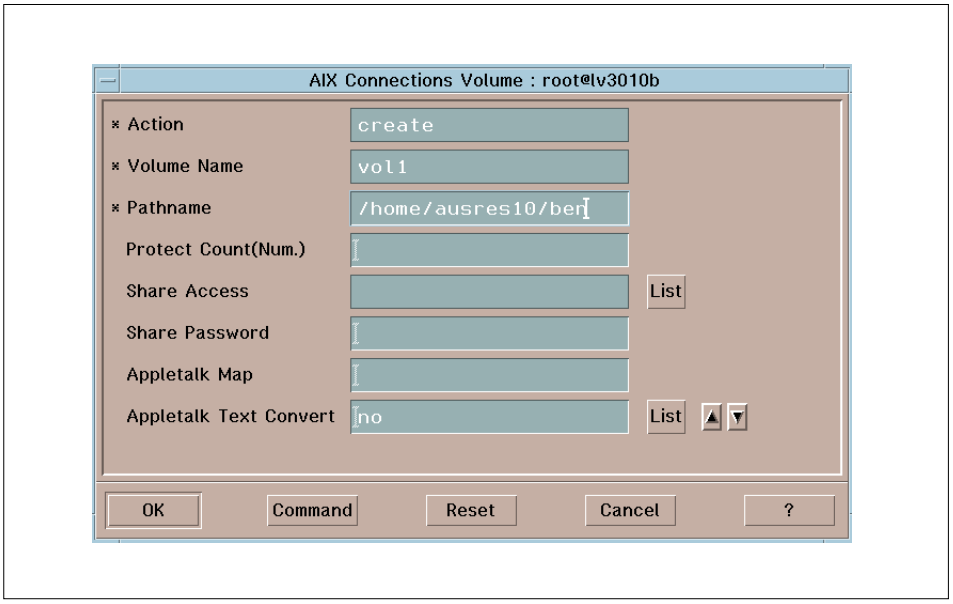


Figure 36. Add a Volume

4. Specify the Pathname, which is the AIX directory you want to share.
5. Click on **OK**.
6. After creating a volume you must create a volume reference, as described in the next section.

4.4.3.5 Creating a Volume Reference

Follow these steps to create a volume reference to the newly-created VOL1 so it will be recognized by the realm:

1. Follow this link:

   Configuration->Volumes->Manage Volume References->*select a realm ->select a service->select a volume*

   In our case the realm is NB Realm, the service is lv3010b, and the volume is VOL1. We will get the following panel:

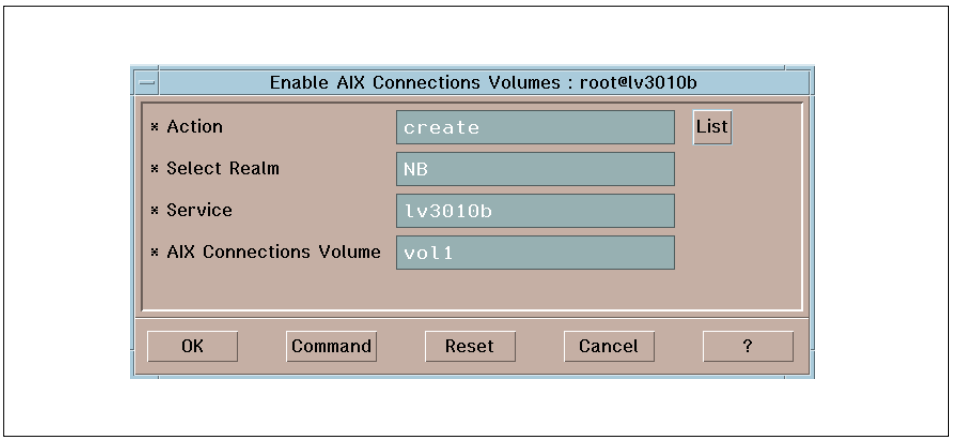


Figure 37. Create a Volume Reference

2. Click on **OK**.

4.4.3.6 Creating/Adding Services

In this section we show you how to create a new service. Please be aware that when you create a terminal service, the only fields you may alter are: Command, Description and Home directory.

If you create a file service and then browse the network using a client's Network Neighborhood, the new service appears as an additional computer server. In this way, having several file services on the same RS/6000 running AIX Connections is equivalent, from a client point of view, to having several file server machines.

Follow these steps to create or add a new service:

1. Follow this link:

   Configuration->Services->Manage Services->*choose a realm*

2. Enter the name of your new service in the Service field. The format of the name is:

   servicename:service_type

   where *servicename* is the name of your new service, and *service_type* is either file, print, term, or nvt. In this example here we create a file service. You get the following panel:

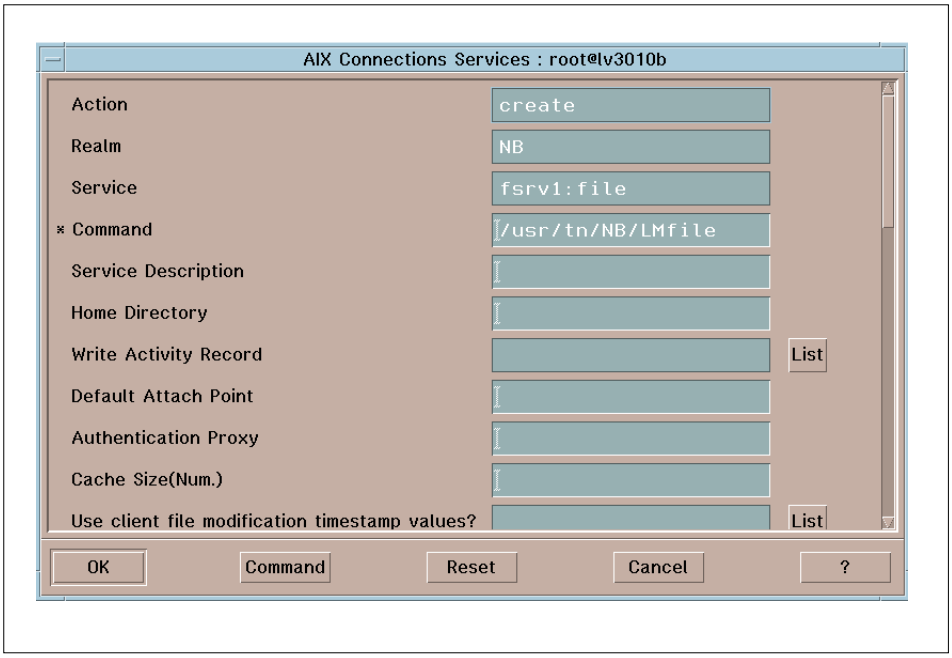


Figure 38. Create Services Panel

The only required field is the Command field.

3. Click on **OK**.

   Your new service will be effective after restarting the AIX Connections server.

4.4.3.7 Creating/Adding Printers

Follow these steps to create a printer in your configuration:

1. Follow this link:

   Configuration->AIX Connections Printers->Configure AIX Connections Printers

2. Select a printer from the pop-up window and then click on **OK**.
3. Click **Modify**.
4. You will get the AIX Connections Printer Configuration panel, where you will be prompted for information in the following:

   AIX Printer Queue

   Spooler Options

Share Access

Share Password

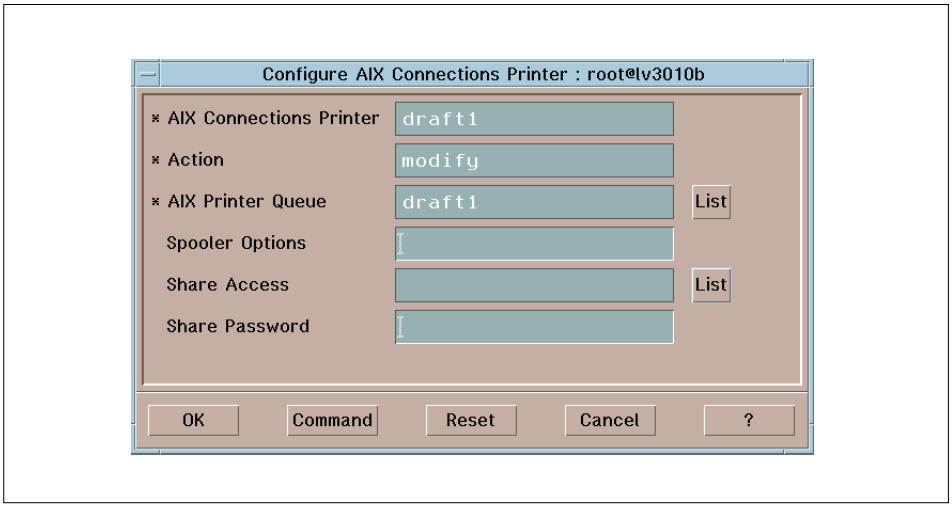


Figure 39. Configure Printer Panel

5. Click on **OK**.
6. Now you have to create a printer reference before the printer can be seen by the clients, as explained in the next section.

4.4.3.8 Adding Printer References

Follow these steps to add printer references:

1. Follow this link:

   Configuration->Enable AIX Connections Printers->*select a realm->select a service->select a printer*

2. You get the following panel:

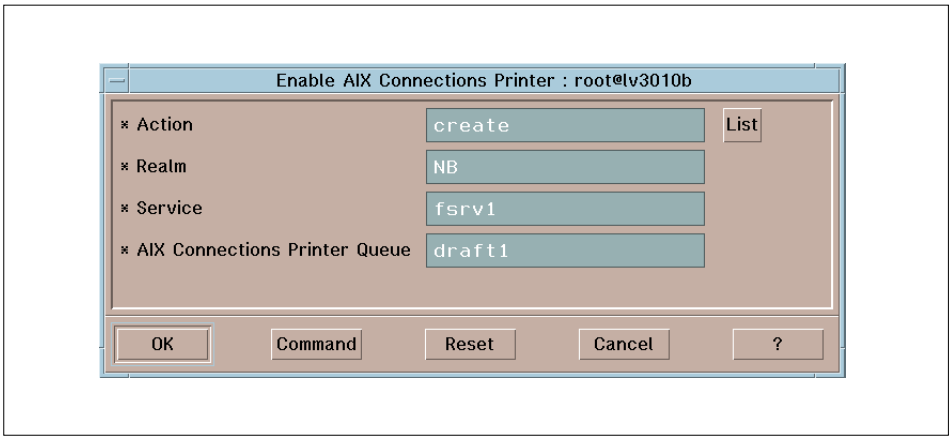


Figure 40. Add Printer References

3. Click on **OK**.

   If there are newly-connected clients, they will be able to see the printers automatically. For previously-connected clients, they will need to reconnect to the server to be able to use this printer.

4.4.4 Configuration Using Web-Based Tool

AIX Connections also allows you to do configuration and administration tasks by using a Web browser, just like TAS. We will show you how to do the Initial Setup and get the server started.

You must start the http daemon using the following command:

```
/usr/tn/totaladmin/W3/bin/tnadmin.sh start
```

Then run your Web browser and open the URL:

http://*hostname:nnnn*

where *hostname* is the hostname of your workstation, in this example it is lv3010b, and *nnnn* is the port number of AIX Connections Admin, which is 7777 by default.

You get the following panel:

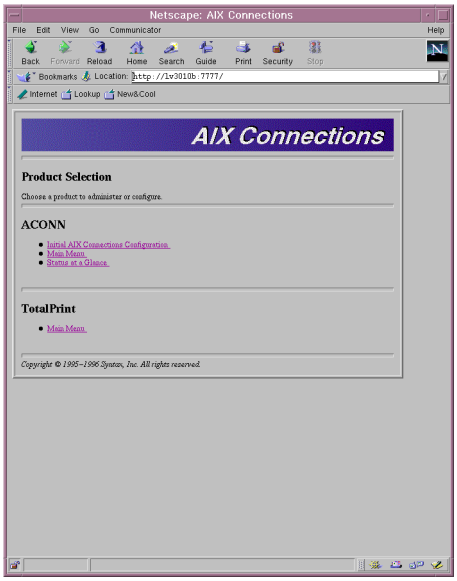


Figure 41. AIX Connections Initial Panel

Then you can configure AIX Connections using the following steps:

1. Select **Initial AIX Connections Configuration.**
2. Log in using your root AIX user ID and password.
3. You get the following panel:

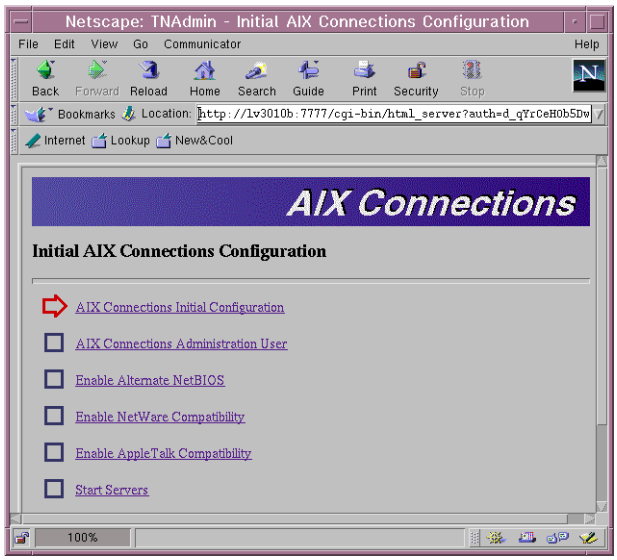


Figure 42. Initial AIX Connections Configuration

4. Select **AIX Connections Initial Configuration**.
5. Select **Check for Superuser** and then click on **OK**.
6. Enter the username and group of the AIX Connections administrator. The default is aconn.
7. Click **Configure Administrative User Info**.
8. In the next panel click on **OK**.
9. You will get the Enable Alternate NetBIOS window. Click **Enable Alternate NetBIOS**, then click on **OK**.

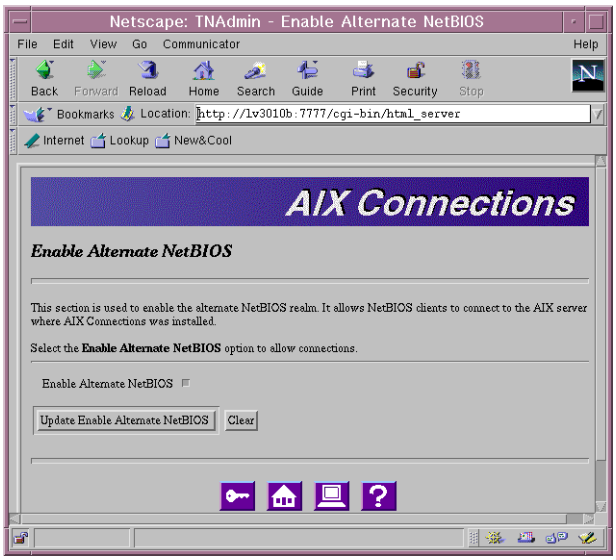


Figure 43. Enable NetBIOS Window

You get the NetBIOS Configuration panel.

10. Click **Update NetBIOS Configuration**.
11. In the next panel click on **OK**.

    The next panel is the Enable NetWare Compatibility panel.
12. Click **Update NetWare Compatibility**, then click on **OK**.

    You get the Enable Appletalk Compatibility panel.
13. Click **Update Appletalk Compatibility**, then click on **OK**.
14. In the next panel, click **Update Start Configured Servers** to start your server, then click on **OK**.

    You will get the Initial AIX Connections Configurations.

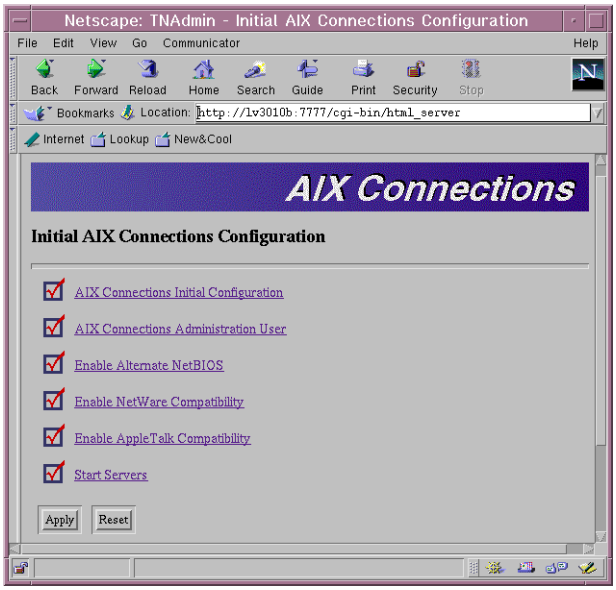


Figure 44. Initial AIX Connections Configuration Window

15.In the Initial AIX Connections Configuration panel, click **Apply**.

16.Click on **OK** in the next panel.

The process is now complete. To get to the AIX Connections Main Menu window, click the **Home** icon.

You will get the AIX Connections Main Menu window, from where you can start all administration and configuration jobs.

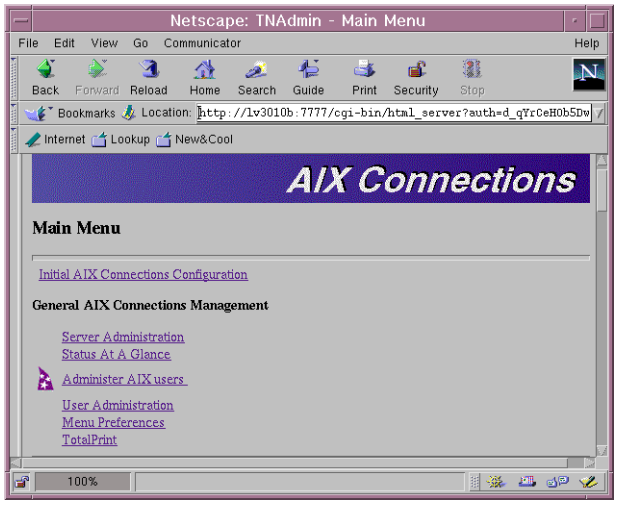


Figure 45. AIX Connections Main Menu Window

Please familiarize yourself with this window. It is self explanatory and very easy to use once you are familiar with it. In the next sections, we show you how to perform AIX Connections tasks using SMIT, but if you prefer to use the Web-based tool, please refer to *AIX Connections Version 4 Administrator's Guide*, SC23-1828-00 for more information.

4.4.5 Post-Configuration Tasks

Before your clients can connect to the server and use the services, there are several post-configuration tasks to be done.

4.4.5.1 Administering AIX Connections Server Password

You must define an AIX user ID in AIX and give authorization to log in through AIX Connections before it can be used to log in from a PC client.

4.4.5.2 Adding an AIX Connections User

Perform the following steps to add an AIX Connections user:

1. Type `smit aconn`
2. Follow this link:

Administration->Add/Change/Delete AIX Connections Password-> Add/Change AIX Connections Password

You will get the following panel:

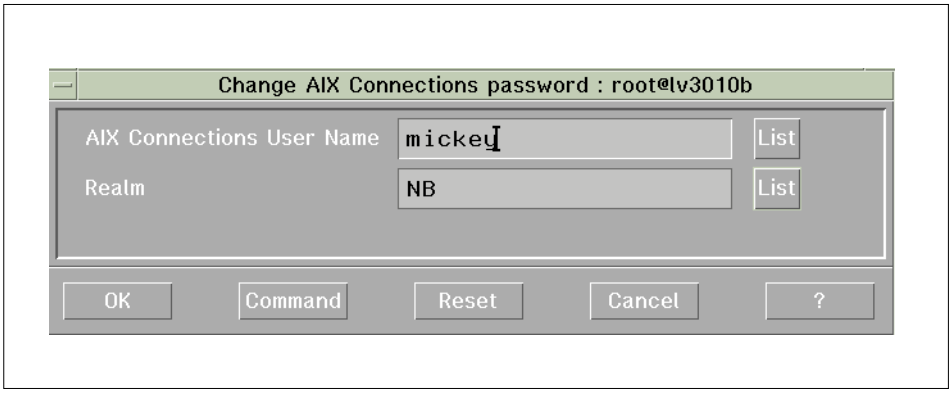


Figure 46. Add AIX Connections Users

Enter an existing AIX user as an AIX Connections user and select the realm needed. You may also select ALL instead of choosing a particular realm. In this way the new password will apply to all realms as well as the AIX operating system.

3. Click on **OK**.

   You will be prompted for the user's password.

4. Click on **OK**.

4.4.5.3 Configuring AIX Connections Licensing Support

AIX Connections contains support for concurrent nodelock licensing. The number of users allowed to connect will be equal to the number of licenses entered in the aclicense utility.

You must install the License Use Management client software. Without it, you will get a default of two clients and will not be able to increase the number of licenses.

Follow these steps to install the License Use Management client software:

1. Start the Nodelock Administration tool with the `/var/ifor/i4nat` command:
2. Select **Products**, then select **New**.

   You will get the New Product window.

3. Select **Import**.

   You will get the Import window.

4. Enter /usr/tn/aconn.lic in the Selection field, then click on **OK**.

   You will get the New Product window.

5. Select **concurrent** in the license field, then click on **OK**.

6. Run the command:

   ```
   /usr/tn/aclicense xxxx
   ```

   In the command above, `xxxx` ranges from 2-1000 licenses. The number of licenses can be changed at anytime by running the `aclicense` command. This change will not take effect until AIX Connections is stopped and restarted.

4.5 Administering AIX Connections

Your AIX Connections is now up and running with the basic default configuration. This section gives a brief explanation about additional administration tasks you may find useful in managing your AIX Connections server.

4.5.1 System Level Tasks

In this section we show you some useful tasks in a system-level basis. You must log in as root to perform any administration tasks, and you will always start from the AIX Connections Main Menu which you can access by using the SMIT fastpath:

```
smit aconn
```

4.5.1.1 Checking the Status of Services

Follow these steps to check the status of services:

1. Follow this link:

   Administration->Server Status

2. You will get a screen similar to the following:

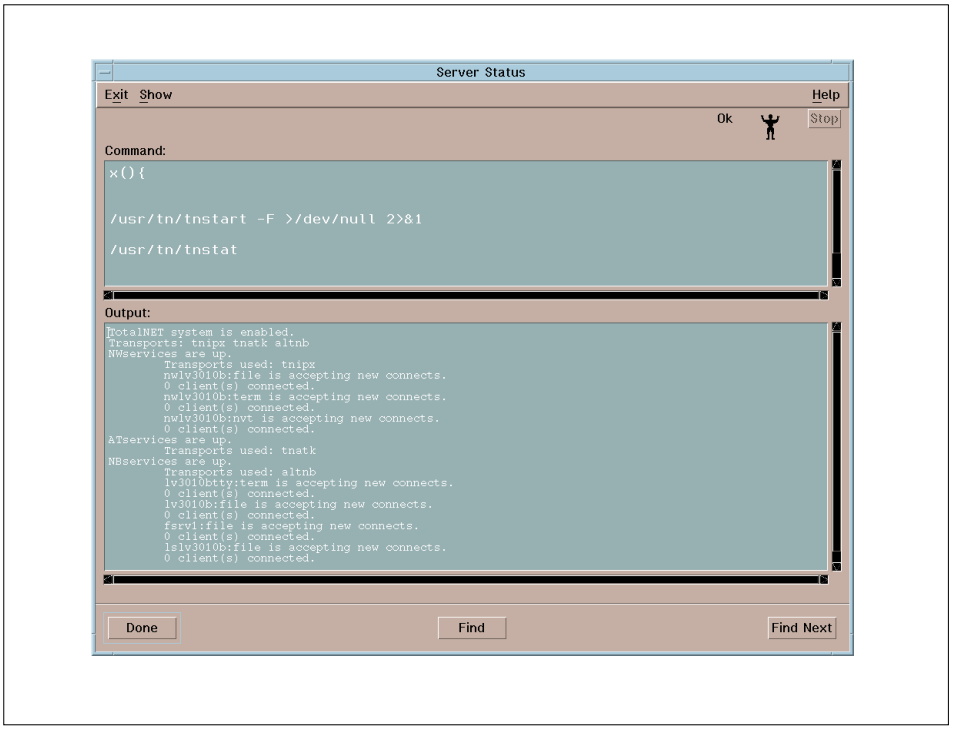


Figure 47. Server Status Output

In the above example we have NB and NW Realms set up. If you only configure for NB Realm, you will have your NB Realm and services up and accepting connections.

4.5.1.2 Starting Services

You have the choice to start a specific realm service or all services in your configuration. Follow these steps to start a service:

1. Follow this link:

   Administration->Start/Stop Realm->Start

2. You will get the Select Realm pop-up screen. Select **ALL** if you want to start all services, or select a specific realm, for instance NB.

Notes

To start a service, you must have LANA configured and NetBIOS running. This was previously done from Quick Start. If for any reason you stop NetBIOS, be sure to stop NB Realm, start NetBIOS, and then restart NB Realm.

4.5.1.3 Starting a Specific Service

You may want to start only one service. For that purpose follow these steps:

1. Follow this link:

   Administration->Start/Stop Servers->Start

2. Select a realm from the Select Realm panel.
3. Choose a service from the Service Name pop-up window.

   Your service is now started.

4.5.1.4 Stopping All Services in a Realm

Follow these steps to stop all services in a realm:

1. Follow this link:

   Administration->Start/Stop Realm->Stop

2. Select a realm from the Select Realm screen, for instance NB.

   Your services in the NB Realm are now stopped.

4.5.1.5 Stopping a Specific Service

Follow these steps to stop a specific service:

1. Follow this link:

   Administration->Start/Stop Servers->Stop

2. Select a realm from the Select Realm panel.
3. Choose a service from the Service Name panel.

   Your service is now stopped.

4.5.2 Realm Level Tasks

Your NetBIOS has now been configured. It must be running before you try to start NB Realm services. In this section we perform tasks from the NetBIOS main menu, which you can access by typing the following SMIT fastpath:

```
smit netbios
```

You get the following panel:

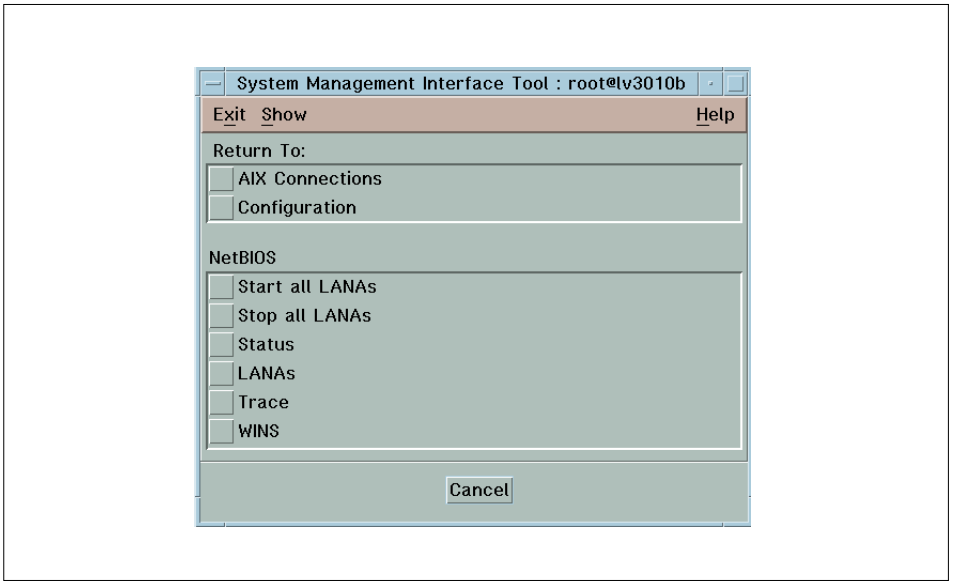


Figure 48. NetBIOS Main Menu

4.5.2.1 Checking NetBIOS Status

Follow these steps to check the status of NetBIOS services:

1. Choose **Status** from the NetBIOS main menu.
2. Choose **LANA**, **Adapter**, or **Sessions** from the Status pop-up panel.

   If you choose LANA, you will get the status of all LANAs.

   If you choose Adapter or Sessions, you will be prompted to choose a specific LANA.

4.5.2.2 Starting NetBIOS

If your NetBIOS is not active, start it now by clicking **Start all LANAs** from the NetBIOS main menu.

4.5.2.3 Starting a LANA

LANA stands for local area network adapter. It is a number to identify the protocol and device used by NetBIOS to make a session.

Follow these steps to start a LANA:

1. Follow this link from the NetBIOS main menu:

LANAs->Start/Stop LANAs->Start

2. Choose one or more LANAs or choose ALL.

   Your LANA is now started.

4.5.2.4 Stopping NetBIOS

To stop NetBIOS, choose **Stop all LANAs** from the NetBIOS main menu.

4.5.2.5 Stopping a LANA

Follow these steps to stop a LANA:

1. Follow this link from the NetBIOS main menu:

   LANAs->Start/Stop LANAs->Stop

2. Choose one or more LANAs or choose ALL.

   Your LANA is now stopped.

4.6 Miscellaneous

This section covers any additional points which are not covered elsewhere in this chapter.

4.6.1 Troubleshooting

In this section we describe how to resolve two common problems that you may have when trying to install and configure AIX Connections for the first time. These are problems we experienced too.

The first problem is that sometimes, when browsing from an NT client, you are not able to see the AIX Connections machine. We have found that you can easily solve this problem by simply configuring the AIX Connections server as a Browse Master. To do so, follow these simple steps:

1. Type **smit aconn** and select:

   Configuration -> **Services** -> **Manage Services** -> **NB**

2. Select the service name.
3. Select **modify**.
4. Set Browse Master to **on**.
5. Select a Browse User (we chose aconn).
6. Optionally, you can select Browse Election Bias and Browse Election Version. Refer to the product documentation (sc23-1828)for help in further configuration.

7. When finished restart the server.

Another common problem is that sometimes you may have problems accessing AIX Connections resources. This means that you see the server, but when asked to log in, you receive a validation error message. One common reason is that AIX Connections by default uses encrypted passwords for user authentication, while NT does not encrypt passwords by default unless Service Pack 3 is installed. So if your NT does not have Service Pack 3 installed, you have to unset encryption from AIX Connections service configuration. To do that, run **smit aconn** and follow these steps:

1. Select **Configuration** -> **Services** -> **Manage Services** -> **NB**
2. Select the service name.
3. Select **modify**.
4. Go to the item **Encrypted Client Password** and set it to **off**.
5. When finished, restart the server.

Another solution to the problem could also be to install the service pack on NT client.

4.6.2 TotalPrint

With AIX Connections we can use a facility called TotalPrint. TotalPrint is an AIX print spooling system that can be accessed via AIX Connections. With TotalPrint, your clients can enjoy features not commonly found in standard AIX print spoolers. They can submit jobs to the TotalPrint print queue and even modify those jobs through your Web browser. All standard spoolers you are already familiar with in AIX, such as lp and lpr, are provided.

AIX Connections relies on the AIX print spooling system to do the printing for its clients. The name of the file printed is provided to the spooler, along with other command line options, by the AIX Connections print daemon.

4.6.3 AIX Connections as a Client

AIX Connections is usually used as a file and printer server. This mean that from an NT machine you access AIX resources. Sometimes, however, you may be willing to access resources exported by an NT server. In this situation the AIX machine is the client. The procedures you use to perform this task are different if you access NT volumes or printers.

4.6.3.1 Accessing NT Volumes

Before accessing NT volume you must log on to an NT machine. To do so, follow these simple steps:

1. Log on as root on AIX.
2. Type `smit aconn`.
3. Select **Client**.
4. Select **Login/Logout**.
5. Fill-in the form, indicating the NT server name, the user to connect (this user must be defined on NT server) and the realm to use (usually NB).
6. When required, enter the password associated with the user on NT server.

At this point you can mount on the AIX machine the volume exported from NT. To do this follow these steps (as root):

1. Type `smit aconn`.
2. Select **Client**.
3. Select **Mount/Unmount Volume**.
4. Fill-in the form, indicating the NT server name, the volume name on the NT machine, the point where you want the volume to be mounted on AIX and the realm (usually NB).
5. Check that the volume has actually been mounted using the AIX `mount` command. You will see a new file system, of type tncfs, mounted on the mount point you specified.

4.6.3.2 Accessing NT Printers

For printing from AIX to an NT machine using NetBIOS protocol, you have to use the `ruprint` utility located in /usr/tn/smb/client directory. Refer to the man page or online documentation provided with AIX Connections for further details on the syntax of the `ruprint` command. On the same directory where you find the `ruprint` command, you can access other client commands that you can execute from AIX to access NT resources, such as getting or putting files, opening a restricted shell, and so on.

4.6.4 Documentation

For more information on AIX Connections, refer to *AIX Connections for Beginners*, SG24-4588-01.

PostScript manuals are available from the AIX Connections CD, by installing the fileset connect.ps.en_US.

After installing the filesets, you will find the manual under the /usr/lpp/connect/doc/en_US AIX directory.

The space required under /usr to install the fileset is about 40 MB.

You can also access AIX Connections documentation using a Web browser, connecting to port 7777 of the AIX Connections server machine. If the httpd is not started, you can start it with SMIT by following these steps:

1. Run **smit aconn**.
2. Select **Administration** -> **Start/Stop AIX Connections HTTPD Daemon** -> **Start**

When finished, you can connect from a browser and access the documentation using these steps:

1. From a browser, select the URL hostname:7777, where hostname is the name of the AIX Connections machine.
2. Select **Aconn Main Menu**.
3. Provide a user and password to access the server.
4. Select **Online AIX Connections Documentations**.

Chapter 5. Novell Network Services for AIX

Novell Network Services 4.1 for AIX (also referred to in this document as NNS) brings Novell's Network Services to the RS/6000 system. With these services, RS/6000 systems running AIX Version 4.2.1 and AIX Version 4.3 can act as servers for products running Novell NetWare on LANs.

5.1 Novell Network Services for AIX Overview

This section provides an overview of the NNS features and a description of how NNS is integrated with the AIX operating system.

5.1.1 History of the Product

Novell is a well-known name in the information technology industry and represents a range of product offerings. Novell software products include server operating systems, network applications and distributed network services. These products enable customers to maintain distributed information resources across computer networks that integrate many different computers, operating systems, applications and devices. Novell provides solutions for LAN and host computer integration. One of these solutions is Novell Cross-Platform Services. Novell Cross-Platform Services (NCPS) is Novell's UNIX operating system solution. NCPS runs on the UNIX system, turns the UNIX system into a NetWare/UNIX server, and uses Novell Directory Services (NDS) to control NetWare client access to the UNIX system resources. Although NCPS is a Novell solution for LAN and host computer integration, Novell does not sell it to customers. NCPS is a source-code product that Novell licenses to manufacturers of host computers such as IBM. IBM ported NCPS to RS/6000 and AIX with the name Novell Network Services 4.1 (NNS) for AIX. We can order this product by using the product number 5765-C95.

5.1.2 Brief Description

Novell Network Services 4.1 for AIX allows NetWare clients to access and use RS/6000 resources as if they were NetWare resources. NNS places NetWare services on the RS/6000, turning the RS/6000 into a non-dedicated NetWare server that provides both host operating and application services and NetWare services. This means that an RS/6000 can continue to run AIX and perform all its former tasks, and simultaneously offer to NetWare clients all the services associated with a NetWare server in a typical NetWare environment.

5.1.2.1 NNS-Supported Clients

Here is the complete list of clients supported by NNS:

- Client for DOS/WIN (VLMs) Version 1.21 or above
- Client 32 for DOS and Windows 3.1x Version 2.11
- Client 32 for Windows 95 Version 2.11
- Client for OS/2 (OS/2 requestor) Version 2.12
- WIN-95 Client, distributed as msnds.exe
- WIN-NT 4.0 NetWare Client and Gateway
- Novell intraNetWare Client 4.11a for Windows NT

In this publication, we will focus on WIN-NT 4.0 NetWare Client and Gateway and Novell intraNetWare Client 4.11a for Windows NT.

5.1.3 NNS Features

To be a complete NetWare server, the server must provide the following basic networking services:

- Novell Directory Services
- File system services
- Print services
- Security services
- Network management
- Communication protocols
- Application Programming Interfaces

5.1.3.1 Novell Directory Services (NDS)

NDS is a global, distributed database that maintains network information and provides access to information across a network. NDS provides access to all network resources, regardless of where they are physically located. Therefore, NetWare users log into the directory tree and, with appropriate rights, have access to any resource on the network.

5.1.3.2 File System Service

File system services permits you to store data in files and organizes these files into directories. The users on the network can access and share the same information. In addition to these basic services, NNS provides the following file system services:

- *Synchronized access*. When more than one client tries to access the same file at the same time, synchronized access prevents file corruption.
- *Name space*. This allows NetWare clients to create file names according to the rules of their workstation's operating system (such as DOS, OS/2, UNIX, Windows NT, Window 95 and Macintosh).
- *Volumes*. NetWare uses a modified hierarchical file system, with multiple root nodes called volumes. NNS allows the file system on AIX to be configured as one volume or up to 64 volumes.

5.1.3.3 Print Services

One of the most important benefits of networking is the ability to share printers. NNS allows the NetWare clients on the network to access printing resources on both NetWare and AIX printers.

5.1.3.4 Security Services

To ensure protection from unauthorized access, NNS offers different types of security services:

- *User account*. NNS ensures secure passwords. Secure password features include encryption and encryption keys that ensure passwords are never sent unencrypted in plain text over the wire.
- *File system*. NNS controls who can access, modify, delete or create files and directories.
- *NDS object*. NNS controls who can manipulate attributes in the NDS database.
- *Print security*. NNS allows you to decide who can use the printers on your network.

5.1.3.5 Network Management

Network management includes the services that allow system administrators to manage servers, clients and network resources. NNS offers the following types of network management services:

- *Instrumentation for Simple Network Management Protocol (SNMP)*. SNMP management consoles can display statistics about the network services.
- *Support for the IPX/SPX diagnostic protocol*. Network management applications can draw physical location maps of the network.
- *Delegation of administrative tasks*. NNS allows you to delegate management responsibilities. For example, the system administrator can make a Novell user an account manager.

5.1.3.6 Communication Protocols

Protocols are part of the networking infrastructure that allow computers to share and exchange information. NSS uses a set of protocols for transmitting information from one computer to another. IPX, IP and SPX are some of these protocols.

5.1.3.7 Application Programming Interfaces

The NetWare API for C is the interface to the C programming libraries for workstation applications. These libraries enable applications to interact with the NetWare server and access NDS.

5.2 Basic Protocol Concepts

> **Note**
>
> In the following section we use two common definitions for network. A single, simple network consisting of a few computers, network boards and one cabling segment is simply called a network. A collection of these simple networks connected with routers, gateways or bridges is called an internetwork.

The following is basic information about the main protocols used by Novell. If the person involved in installing Novell Network Services 4.1 for AIX on RS/6000 is skilled with Novell, they can skip this section. Otherwise, it is useful to read this part before installing the product. Protocols are part of the networking infrastructure that allow computers to share and exchange information. To understand any other networking service such as NDS, file service or print service, we must have some knowledge of the services that transport the information across the network.

5.2.1 IPX Protocol

The Internetwork Packet eXchange (IPX) protocol is a connectionless, datagram service protocol. It is a connectionless protocol because IPX does not require a connection to deliver packets and can deliver a packet to any node on the network of which IPX has the address. IPX is a datagram protocol because it does not require an acknowledgment for each packet sent and it does not guarantee that a packet was delivered. Other NetWare protocols that provide services, such as guaranteed service and packet sequencing (SPX/SPXII), service advertising (SAP), routing (RIP), and NCP (NetWare Core Protocol) are built on top of IPX. IPX provides full internetwork addressing. It defines network and socket numbers while using

the node addressing scheme of the network interface hardware for clients. IPX provides routing, transport and addressing services. As LAN drivers for the network boards deliver packet to IPX, IPX uses RIP to determine the route for packets outbound to other networks and uses socket numbers to determine the application on the local node. An IPX address identifies each network, each computer on the network, and the process or application in the computer that sent the packet. Two computers cannot share an address, each must be unique. An IPX address includes three components: the network address, the node address and the socket number. The network address identifies a specific network or LAN on an IPX internetwork (this is the external address). The node address identifies an individual computer on a network (this is the internal address). For a client workstation, the node address is defined by networking hardware and is usually factory-set in the hardware or firmware of the network board. For server workstations, NetWare configures a logical node address for the internal network. For the networks that the server attaches to, NetWare uses the node address that is factory-set in the hardware or firmware of each network board. Each NetWare server has at least two node addresses, one for the internal network and one for the network board. If the NetWare server is acting as a router because it has more than one network board, the NetWare server will have three or more node addresses.

5.2.2 RIP Protocol

The routing information protocol (RIP) maintains the routing information that IPX uses to obtain the most efficient route to a destination network on an internetwork. RIP does not do the actual routing of the packets, IPX performs those tasks. RIP's responsibility is to maintain an up-to-date router information table and to respond to routing information requests. A routing information table is a dynamic map of the networks and routers on an internetwork. When a router first come up, it uses RIP over IPX to broadcast information about itself to the other routers on its network. The information is passed to other routers until all routers on the internetwork know about the new router.

5.2.3 SAP Protocol

The Service Advertising Protocol (SAP) provides a way for service nodes, such as file servers, print servers and gateway servers, to register their services and addresses in a server information table and have these services advertised across an internetwork. All nodes on the network that supply SAP services have a SAP agent. For NNS servers, the SAP daemon (SAPD) is the SAP agent. All SAP agents are responsible for keeping their server information tables up-to-date and for responding to service queries. The

major task for SAP agents is responding to queries about available services. The IPX protocol requires the sending node to know the address of the receiving node. To obtain the IPX address, the sending node can query a SAP agent for the address of a particular server or for a list of servers providing the needed service. Keep in mind that network addresses can be obtained from a SAP agent or from a NetWare server's object database (Novell Directory Services). Using a SAP agent is conceptually similar to using the yellow pages of the telephone directory. All services are grouped according to types of services. The SAP agent provides faster access to information about types of servers than does the NDS database. Using NDS is like using the white pages in the telephone directory. NDS provides faster access to information about a particular server than the SAP agent.

5.2.4 SPX and SPX II Protocol

The Sequence Packet Exchange protocol (SPX) is a guaranteed delivery, connection-oriented, sequenced transport protocol. SPX is a reliable protocol because it guarantees packet delivery to the destination endpoint, and when delivery is not possible, it notifies the sender that the packet could not be delivered. If SPX encounters a data transmission error, it retries a given number of times before closing the connection and notifying the connection user. SPX also notifies the user if a disconnection indication is received from the remote connection endpoint. SPX is a connection-oriented protocol because both the sending and receiving endpoints maintain connection information about the other endpoint. SPX is a sequenced protocol because each endpoint knows the number of the next expected packet. SPX also provides flow control, which means it regulates the speed with which packets are sent and received by both the sending and receiving processes. SPX II is the name of Novell's enhanced version of the SPX protocol.

5.2.5 NCP Protocol

The NetWare Core Protocol (NCP) is the name of the protocol that NetWare servers use to respond to client requests for network services. It is built on top of IPX. NCP provides different protocol services, connection and session, including guaranteed delivery, flow control and sequencing. A NetWare client builds an NCP packet containing all the required information and sends it via the network to a NetWare server. The NetWare server reads the request, executes the task, and returns the results to the client.

5.3 Novell Directory Services Terminology

Novell Directory Services (NDS) is a database of network information. It is called a database because NDS has powerful facilities for storing, accessing, managing and using the information it contains. The database is called the directory or the directory tree because it stores information like a phone directory and organizes the information like the directory structure in a file system. The NDS structure is similar to the structure of a NetWare file system. Both have a root:

- For the NetWare file system, the root is a volume with a given name.
- For NDS, the root is a tree with a given name.

Below the root, both organize their objects in a hierarchical tree:

- A volume stores files in directories and subdirectories.
- NDS stores network resources as users, groups, servers, printers, queues and so on in containers and subcontainers.

In the following sections we examine a simple example of tree, relating to our installation of the product. Figure 49 illustrates our example, a directory tree called NDS1.

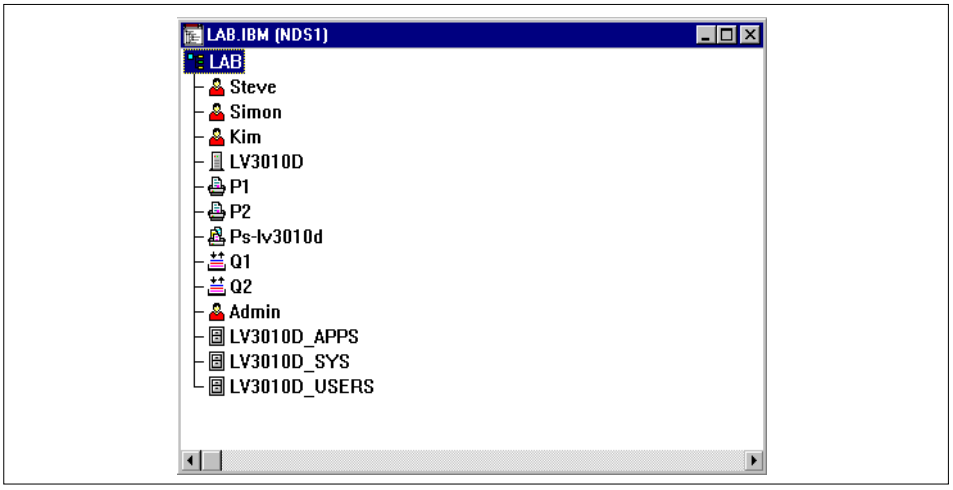


Figure 49. NDS1 Directory Tree

The NDS1 tree has one organization container called IBM. The IBM container contains organization unit container LAB, and LAB has been expanded to

show some of the objects it contains. A directory tree contains three types of objects:

- Root object (directory tree name)
- Container objects
- Leaf objects

The root object is placed at the top of the tree during the installation of NDS on the RS/6000 server. Container objects are created under root and can hold other container objects and leaf objects. Leaf objects represent network resources and do not contain any other object.

5.3.1 Container Objects

Container objects hold (or contain) other directory objects. There are four types of container objects:

1. **Country (C)** The country objects designate the countries where your network resides and organizes other objects within the country. Country objects are optional.
2. **Locality (L)** The locality object designates the location where this portion of your network resides and organizes other objects within the location. Locality objects are optional.
3. **Organization (O)** An organization object helps us organize other objects in the directory tree. Every directory tree must contain at least one organization object.
4. **Organizational unit (OU**) An organizational unit object helps us organize leaf objects in the directory tree. Organizational unit objects are optional.

5.3.2 Leaf Objects

Directory leaf objects are objects that do not contain other objects. These represent network resources as users, servers, printers, and groups.

5.3.2.1 Object Properties

Each type of object (such as users, servers or printers) has properties that store information about that object. The NDS utility allows us to search for objects that have specific property values. We can also request information about a specific object.

5.3.3 Object and Property Rights

NDS uses two categories of rights:

- Object rights
- Property rights

These rights determine what we can do within the directory tree. Because the directory tree is a hierarchical structure, rights assigned in the directory tree flow down through the tree. While object rights control access to an object as an entity, property rights control access to the information stored in an object's properties.

5.3.3.1 Object Rights

Object rights control who can see the objects in the tree and what trustees of the object can do to with the object. A trustee can be a user who has been granted rights to the object. Object rights allow a user to browse, create, delete and rename an object.

5.3.3.2 Property Rights

Property rights allow trustees to read, compare or modify the object property values. To see the information in an object's properties, trustees must have the correct property rights.

5.3.4 Context and Names

In Novell Directory Services, context refers to the location of an object in the directory tree. The NDS context is a list of the containers that contain the object, from the root of the tree to the object's parent container. Context is important because NDS objects are identified by their relative location in the directory tree. An NDS context starts with the object's parent container and list the subsequent containers in ascending order to the root, using periods as separators. An example of context for a user is shown below:

```
OU=LAB.O=IBM.
```

Names in the directory tree have two forms: typeful and typeless. A typeful name includes the name type (OU,O,C,CN) of each object. A typeless name excludes the name type for each object. Table 1 is an example of naming convention for the user KIM.

Table 1. Naming Convention

Form	Example
Typeless	KIM.LAB.IBM.
Typeful	CN=KIM.OU=LAB.O=IBM.

CN designates the common name of the leaf object, OU is the organizational unit name, O is the organization name and C the country name.

5.3.5 NNS Integration with RS/6000

The operating environments of native NetWare and NNS are very different. Native NetWare boots from DOS and dedicates the system to running only NetWare. NNS boots from AIX and allows the system to offer both AIX and NetWare services. NNS does not remove AIX, but instead integrates its services into AIX operating systems. Figure 50 shows the differences between these two methods by tracing a file request through a native NetWare server and an NSS server.

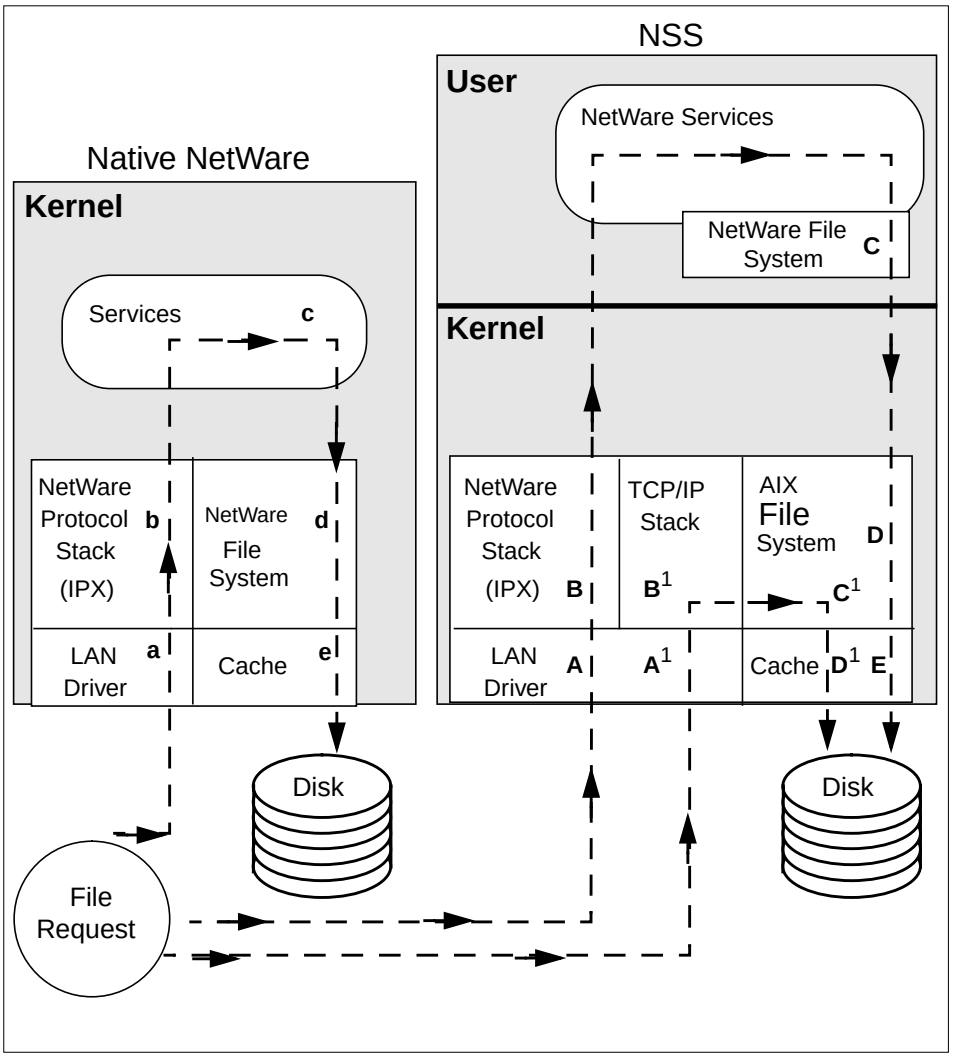


Figure 50. Native NetWare and NNS Architectures Compared

The LAN driver determines where packets are sent for processing. On native NetWare, file requests are automatically handed to the NetWare protocol stack (IPX) for processing (a-b-c-d-e in Figure 50). If the request is submitted to an NSS server, the LAN driver determines whether the file request is for the NetWare protocol stack or for another protocol, such as TCP/IP (A-B or A^1-B^1 in Figure 50).

- If the packet is for the TCP/IP stack, AIX controls the packet. Usually, the packet goes to the AIX file system (A^1-B^1-C^1-D^1 in Figure 50).
- If the packet is for the NetWare protocol stack, the LAN driver hands it to the NetWare stack, and the NetWare modules direct its path to the file requested (A-B-C-D-E in Figure 50).

It is important to note that a file request on the NSS goes through both the NetWare file system and the AIX file system before it can find the file either cached or on the hard disk. The NNS server has no direct access to the RS/6000's hardware because the AIX operating system maintains control of all hardware resources.

5.3.5.1 Process Architecture

On RS/6000s, NNS runs a series of drivers and application programs. These modules divide into two packages: transports and service. Figure 51 illustrates the major modules of these two packages.

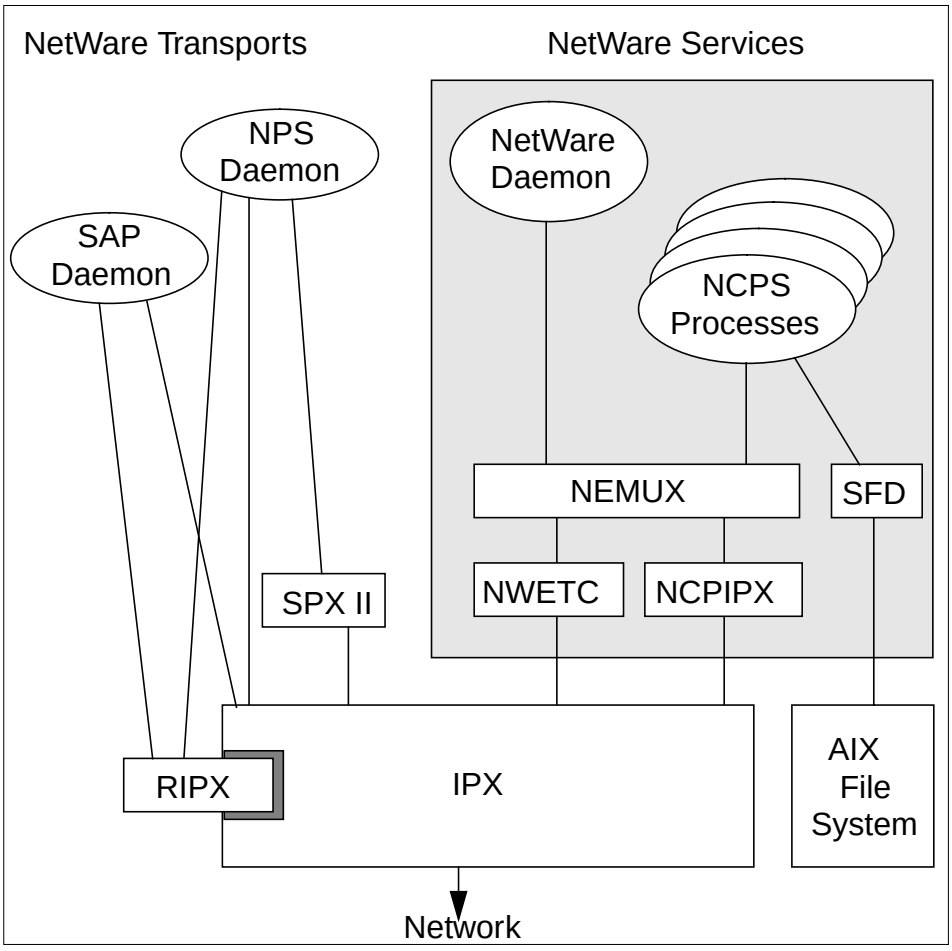


Figure 51. Core NNS Modules

NNS has two controlling daemons:

- NetWare Protocol Stack (NPS) daemon is the controlling daemon for the NetWare transports. It is responsible for linking kernel drivers and starting daemons required to set up IPX communication services.

- NetWare daemon is the controlling daemon for the NetWare services. It is responsible for linking kernel drivers and starting daemons required to set up NNS services.

5.3.6 Licensing System

NNS uses a client/server licensing model based on the iFOR/LS management system. The iFOR/LS server-based licensing scheme contains a license server that maintains a license database. The license database contains the availability of licenses and maintains a count of product usage. NNS uses concurrent-use licenses, which allow users to access the program product from any machine in the network. The number of users that can use the product is limited by the number of user features acquired for the licensed program. Additional connections beyond the amount purchased are not allowed (server failure). The customer should make sure that the proper number of connects are ordered for the environment. You can order Novell Network Services 4.1 for AIX (5765-C95) Server function or SCALE function. The Server function includes a two-user license. If you order the Server function and require the SCALE function (or replication), you must order the SCALE feature separately. If you order five connects or more, you are automatically entitled to use the SCALE function and therefore are not required to order it separately. Connect feature codes are additive after you order the first five connects.

5.4 Installation and Configuration Example

This section provides an example of how to install and configure NNS for AIX so that RS/6000 will appear to the network as a NetWare server. In this example we perform the following tasks:

- Install NNS for AIX code in accordance with its license policy.
- Configure NNS for AIX.
- Start NNS for AIX processes.

If this is the first time you have installed NNS for AIX, it is recommended that you read this entire section before starting. This example explains the key decisions that must be made during installation, as well as the steps taken to install NNS.

Note

We must log in as root to perform all installation and configuration tasks.

5.4.1 Reference Material

Information on installing and customizing Novell Network Services 4.1 for AIX can be found in the following documents, available on the product CD-ROM.

- *Novell Network Services 4.1 for AIX Quick Beginnings* (SC23-4131-00)
- *Novell Network Services 4.1 for AIX Concepts*
- *Introduction to NetWare Directory Services* (SC23-4132-00)
- *Novell Network Services 4.1 for AIX System Messages*
- *Novell Network Services 4.1 for AIX Supervising the Network* (SC23-4140-00)
- *Novell Network Services 4.1 for AIX Printing Services*

5.4.2 System Requirements

The following list details the system requirements for using NNS:

- NNS runs on AIX Version 4.2.1 or AIX Version 4.3. The iFOR/LS License System must be installed.
- RS/6000 workstation with a minimum of 32 MB of memory. (It is recommended that the server has 64 MB of memory.)

An RS/6000 workstation needs 200 MB of hard disk space to install NNS. It is recommended that the server has 1 GB of disk space dedicated to the NNS environment. The installation process requires two dedicated file systems:

- **/ncps** requires at least 150 MB of disk space to hold the SYS volume. This file system is the most critical. We have to size it to contain everything we need clients to access.
- **/etc/ncps/control** requires at least 30 MB of disk space.

Note

The installation process will create these two file systems in rootvg. If we want these two file systems to exist in another volume group, we need to create them before installing NNS. The name of the file systems cannot be changed.

5.4.3 Installation of the Novell Network Services for AIX Code

NNS is composed of the following filesets:

ncps.base.api NNS Services API

ncps.base.cmd	NNS Commands
ncps.base.kernel	NNS Kernel Support
ncps.base.ldap	NNS LDAP Support
ncps.base.nls	NNS Base NLS Support
ncps.base.smit	NNS SMIT Panels
ncps.html.en_US.nns	NNS Guides
ncps.sys.com	NNS Common Client Support
ncps.sys.login.com	NNS Common Client Login
ncps.sys.login.nls	NNS Client NLS Support
ncps.sys.public.com	NNS Public Commands
ncps.sys.public.dos	NNS DOS Client Support
ncps.sys.public.nls.com	NNS Common Client NLS Support
ncps.sys.public.nls.dos	NNS DOS Client NLS Support
ncps.sys.public.nls.os2	NNS OS/2 Client NLS Support
ncps.sys.public.nls.win	NNS Windows Client NLS Support
ncps.sys.public.os2	NNS OS/2 Client Support
ncps.sys.public.win	NNS Windows Client Support
ipx.base.api	IPX/SPX API Support Files
ipx.base.lib	IPX/SPX Libraries
ipx.base.smit	IPX/SPX SMIT Panels
ipx.msg.en_US	IPX/SPX Protocol Suite
ipx.base.rte	IPX/SPX Protocol Stack Runtime
ipfx.rte	Information Presentation Facility Runtime
ipfx.msg.*	Information Presentation Facility Messages

Note

The NNS and *ipx.rte* software packages are mutually exclusive. We must uninstall *ipx.rte* before installing NNS and the *ipx.base* software package.

We have to install all the filesets except for the *ncps.sys* filesets related to clients that we do not have in our network. During the installation process, 20 MB of disk space in /usr file systems will be require. One group, *nwgroup*, will

be create. Four users belonging to nwgroup will be created: *nwroot*, *nwprint*, *nwldap* and *nwuser*. The NNS for AIX code is installed in the same way as any other licensed program products (LPP):

1. Log in as root and type:

   ```
   smitty install_latest
   ```

2. Press **F4** and select the CD-ROM drive from the list.
3. To install NNS, leave the defaults on the installation panel and press **Enter**.

After installation, you may need to reboot your machine if you are using a token-ring adapter and DLPI support.

5.4.4 User License Configuration

We must configure the license server before configuring the NNS server. Refer to Chapter 6 of *Novell Network Services 4.1 for AIX Quick Beginnings* (SC23-4131-00) for details about license server configuration. We must configure the number of user licenses that the NNS server will obtain at start time:

1. Type `smit ncps` to get the following screen:

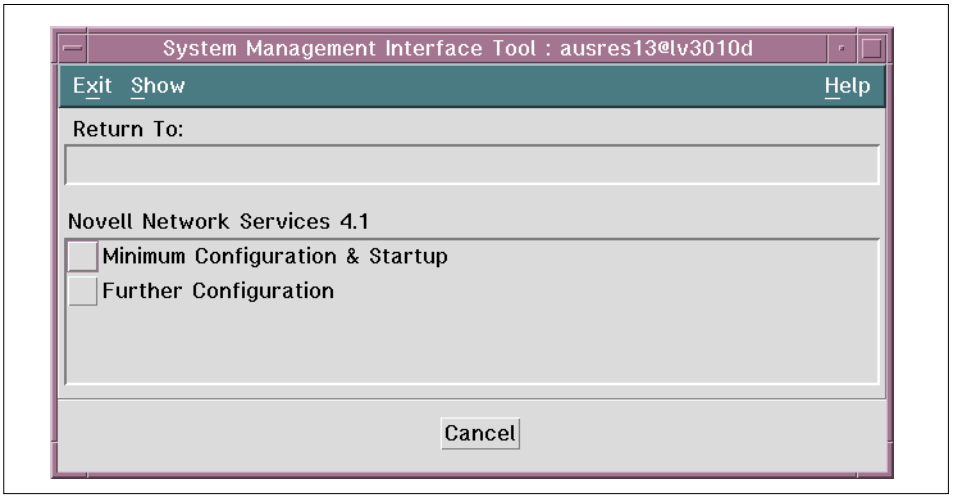


Figure 52. Output of the Command smit ncps

2. Select **Further Configuration** to get the following screen:

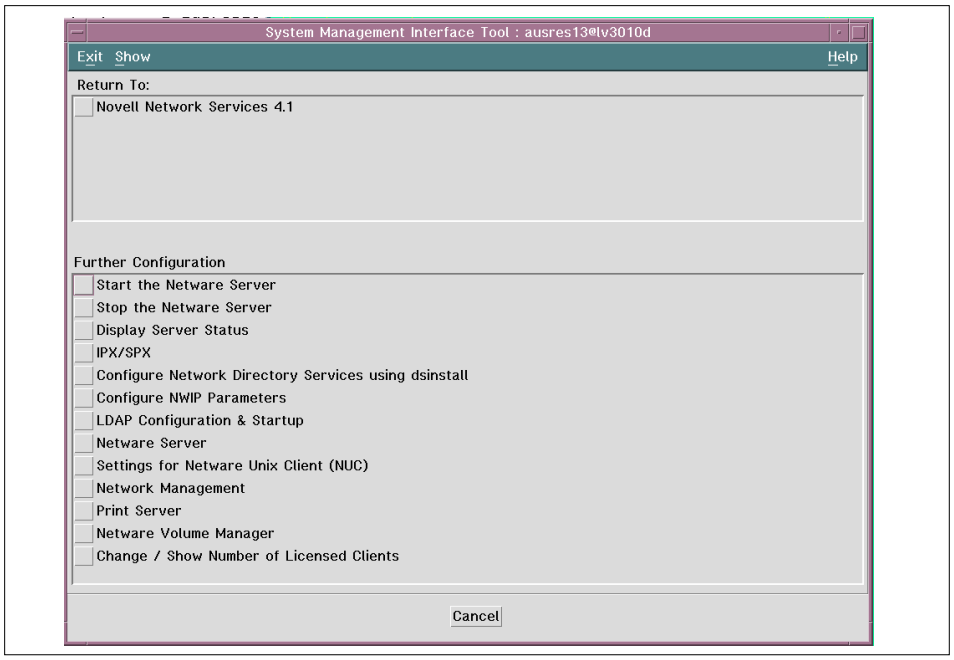


Figure 53. SMIT Panel

3. Select **Change/Show Number of Licensed Clients**, and you will get the following screen:

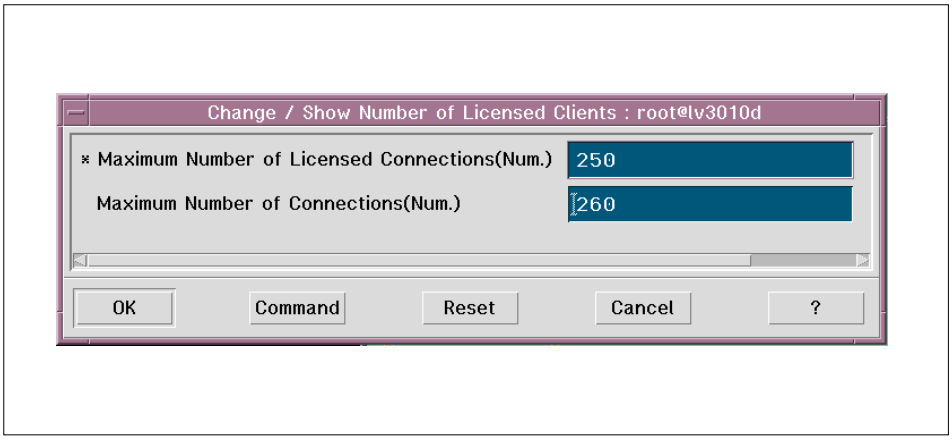


Figure 54. Change Show Number of Licensed Clients

In the field Maximum Number of Licensed Connection, you must enter the maximum number of licensed clients in accordance with the licenses that have been purchased. If you do not enter a value, by default, two licenses will be obtained by the NNS server from the iFOR/LS server at startup time. The number of connections specifies the size of the internal connection table. Since both user licensed-connections and directory services connections use this table, you have to configure the table for at least ten more than your maximum number of licenses. We can increase this number if we have a large directory tree or we receive messages that the connections table is full. The default value is 50. When the NNS is initialized, the server writes a log entry into the /var/ncps/osm file. The entry is shown below:

```
SERVER-4.10-608: License file processing complete. Total number of licensed
connections is 250.
```

Note

If you make any changes to the number of licensed connections, you must stop and restart the NNS server.

5.4.5 NNS Configuration and Startup

Begin by configuring your IPX LAN on your NNS server. To do this, at the AIX command line type:

1. `smit ncps`

   The following panel appears:

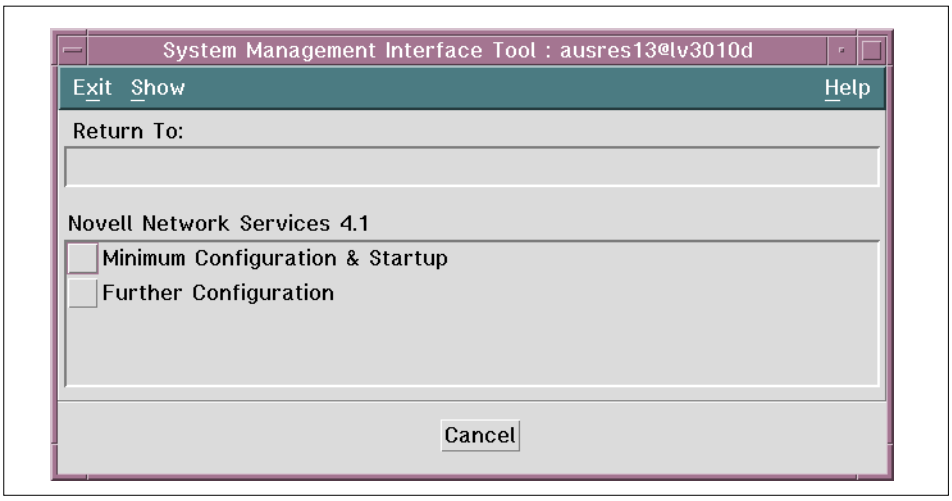


Figure 55. Output of the Command smit ncps

2. Select **Further Configuration -> IPX/SPX -> LAN -> Add LAN.** The following panel appears:

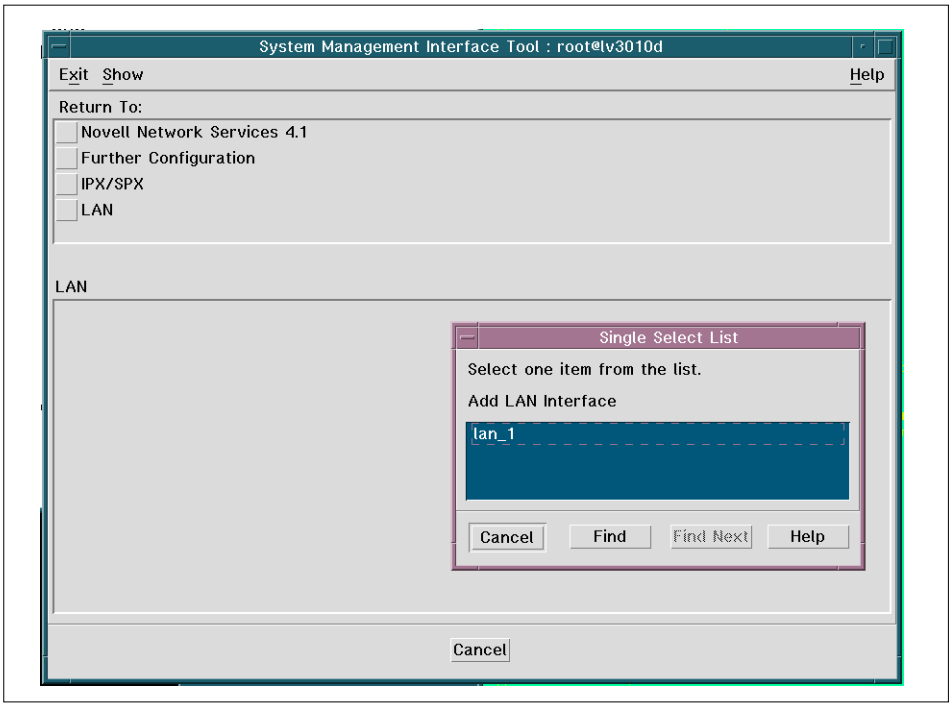


Figure 56. Configuring the LAN

3. The example show us **lan_1**. This is because it is the first IPX/SPX LAN configured on the system. The Add a LAN Interface panel is shown below:

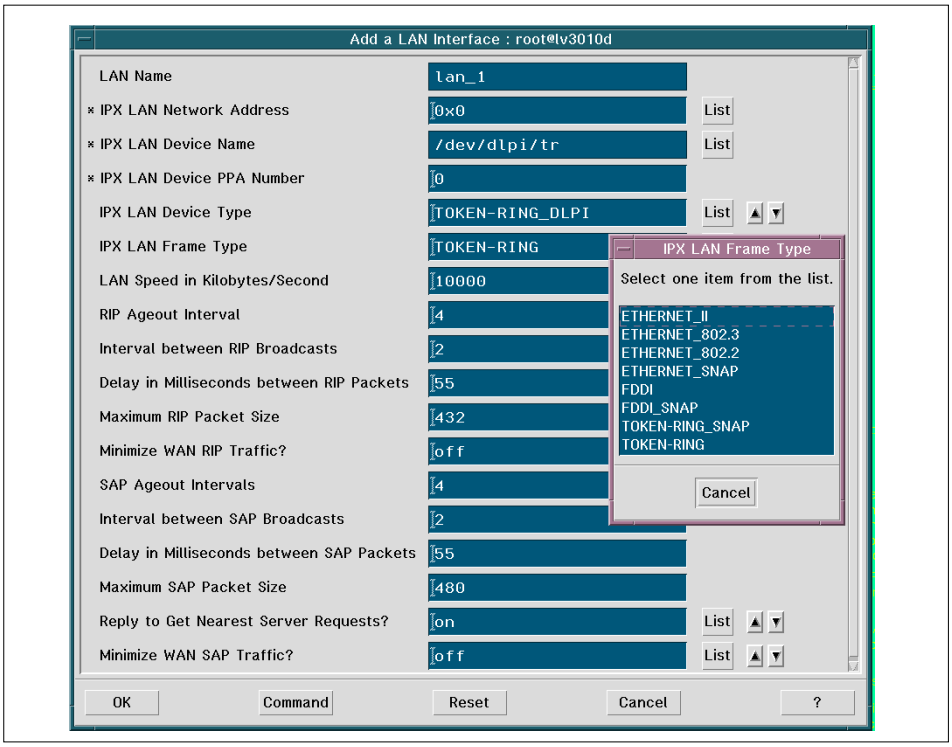


Figure 57. Add a LAN Interface

4. The IPX LAN Network Address specifies the IPX external network number for the cabling system to which the network adapter is attached. The default value (0) signifies that the network is not configured. This parameter is a 4-byte hexadecimal number unique for each LAN on the network. This parameter must be specified.
5. Verify that the IPX LAN Device Name, IPX LAN Device Type and IPX LAN Frame Type are valid. Select **List** to obtain a list of valids type.
6. Check the IPX LAN Device Physical Point of Attachment (PPA). The PPA number must match the interface that you want to configure. In this example the value `0` is related to the tr0 interface on the tok0 device.
7. Press the **Enter** key to save changes.

Note

The administrator must stop and start the NetWare server if any additional LANs are created or if any modifications are made to an existing LAN.

Now you are ready to do the Minimum Configuration and Startup of the NNS server. At the AIX command line type:

1. `smit ncps`

   The following panel is displayed:

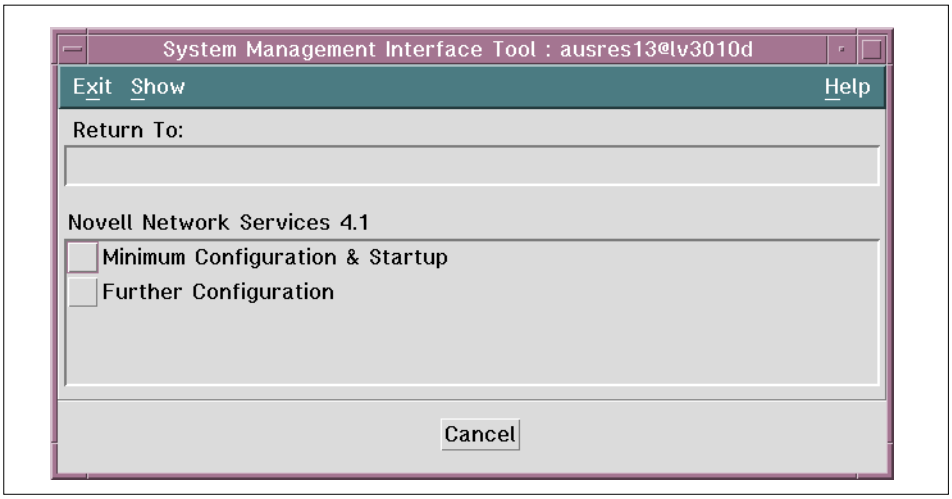


Figure 58. Output of the Command smit ncps

2. Select **Minimum Configuration & Startup.** The following panel is displayed:

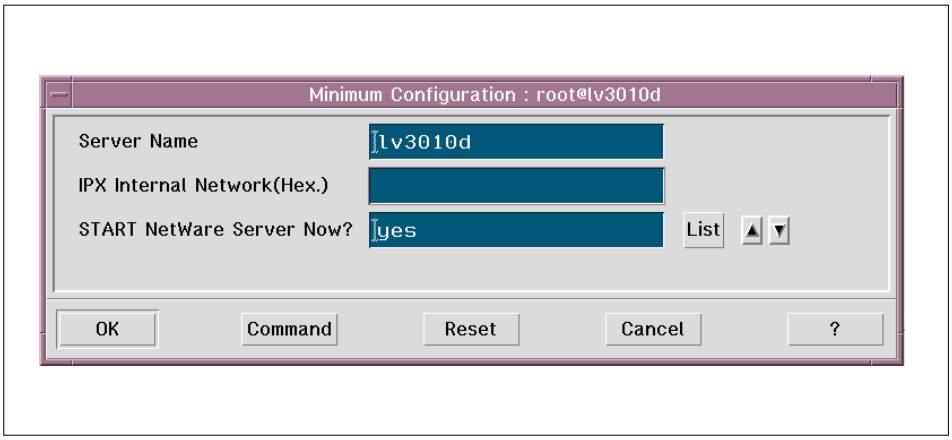


Figure 59. Minimum Configuration

3. The Server Name parameter controls the name under which all IPX services are advertised on the network. By default, NNS displays the system's hostname in the Server Name field, although if needed, you can change it.
4. The IPX Internal Network parameter provides a single network address with access from multiple LANs. This network address must be unique from all other assigned network addresses on the IPX internetwork.
5. The Start NetWare Server Now field defaults to Yes.
6. Press the **Enter** key to save changes and begin the configuration process.

Note

The configuration process log file is /var/ncps/inform.log.

At the end of the process we are able to configure Novell Directory Services (NDS). Directory services are databases of information with powerful facilities for storing, accessing, managing and using different kinds of information about users and resources in computing environments. To configure NDS at the AIX command line, type:

1. `smitty ncps`

   The following panel appears:

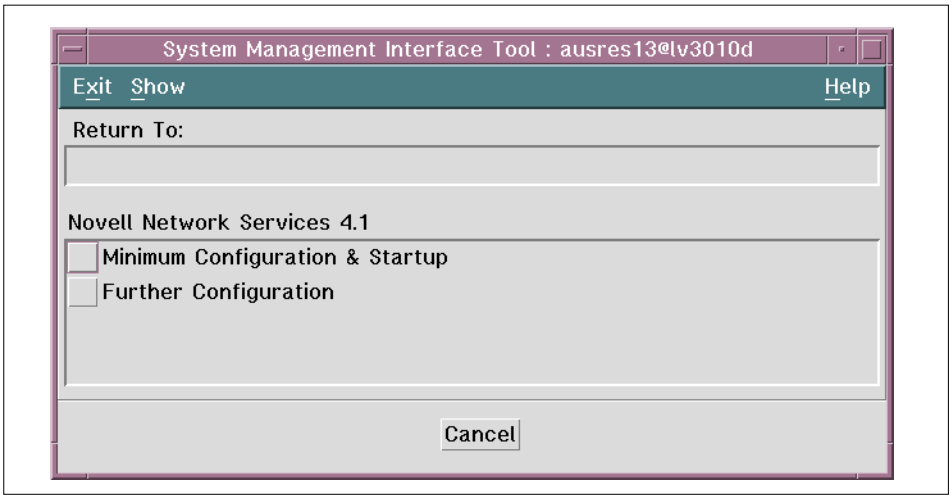


Figure 60. Output of the Command smit ncps

2. Select **Further Configuration -> Configure Network Directory Services using dsinstall.** The following panel appears:

```
        1) Install a new SANDS tree
        2) Install a new SCALE tree
        3) Add a new server into an existing SCALE tree
        4) Upgrade this SANDS server/tree to SCALE
        5) Remove Directory Services from this server
        6) Upgrade mounted volumes into the Directory
        7) Exit

Enter option number:
```

NDS is a database of network information. The database is called a directory tree because it stores information like a phone directory and organizes the information like the directory structure in a file system. Depending on what type of server license is purchased, you can either install a Standalone NDS (SANDS) tree or a Scalable NDS (SCALE) tree:

- SANDS -> Stand-alone mode that allows one NetWare server and any number of network objects into the tree. No other NetWare servers can be added to the directory tree and the NDS database cannot be partitioned and distributed. With a SCALE license certificate, a SANDS server can be upgraded to a SCALE server.
- SCALE -> Scalable mode that allows multiple NetWare servers into the tree and any number of network objects. Each NetWare server added to the tree requires a SCALE license certificate. The NDS database can be partitioned and distributed.

You must enter the option number related to the type of tree, in accordance with the license mode purchased.

5.4.5.1 SANDS Mode Server

If you select option 1, `Install a new SANDS tree`, you must answer the following questions:

```
        1) Install a new SANDS tree
        2) Install a new SCALE tree
        3) Add a new server into an existing SCALE tree
        4) Upgrade this SANDS server/tree to SCALE
        5) Remove Directory Services from this server
        6) Upgrade mounted volumes into the Directory
        7) Exit

Enter option number: 1

Enter the NDS Tree Name: NDS1

Enter the Server Context (e.g. O=cc): OU=LAB.O=IBM

Enter the ADMIN password:

Re-enter the ADMIN password:
```

1. The NDS Tree Name must be unique across the internetwork. In our example it is `NDS1`.
2. The Server Context is related to the structure of the tree. The directory tree name is automatically placed at the top of the tree during installation of NDS. Branches of the directory tree consist of container objects. Container objects can hold other container objects. Leaf object are the ends of the branches and do not contain any other objects. NDS recognizes three different kind of container objects: C (country), O

(organization), OU (organization unit). We have to enter the context by starting with the deepest-nested object and ending with the root object. In this example, to install the server in the OU container object named LAB under the O container object named IBM, enter:

```
OU=LAB.O=IBM
```

3. Type the password for the user ADMIN and press the **Enter** key, then retype the password to confirm it. At this point, the dsinstall utility tries to create the SANDS tree. If the operation is successful, dsinstall displays the message:

```
Number of volumes installed into the Directory: 1 (DSINSTALL-4.2-139)

Installation of Directory Services on this server successful. (DSINSTALL-4.2-26)


This server's clock is network synchronized. (DSINSTALL-4.2-83)


Press Enter to continue.
```

4. We recommend that you record the information (tree, context and password) supplied during configuration. You need the information the first time you log in to the server as user ADMIN.

5.4.5.2 SCALE Mode Server

If you select option 2, `Install a new SCALE tree`, you must answer at the following questions:

```
       1) Install a new SANDS tree
       2) Install a new SCALE tree
       3) Add a new server into an existing SCALE tree
       4) Upgrade this SANDS server/tree to SCALE
       5) Remove Directory Services from this server
       6) Upgrade mounted volumes into the Directory
       7) Exit

Enter option number: 2

Enter the NDS Tree Name: NDS1

Enter the Server Context (e.g. OU=aa.OU=bb.O=cc): OU=LAB.O=IBM

Enter the ADMIN password:

Re-enter the ADMIN password:

Add a SCALE License Certificate? (y/n)
```

1. The NDS Tree Name must be unique across the internetwork. In our example it is `NDS1`.
2. The Server Context is related to the structure of the tree. The directory tree name is automatically placed at the top of the tree during installation of NDS. Branches of the directory tree consist of container objects. Container objects can hold other container objects. Leaf object are the ends of the branches and do not contain any other objects. NDS recognizes three different kind of container objects: C (country), O (organization), OU (organization unit). We have to enter the context by starting with the deepest-nested object and ending with the root object. In this example, to install the server in the OU container object named LAB under the O container object named IBM, enter:

   ```
   OU=LAB.O=IBM
   ```

3. You have to type the password for the user ADMIN and press the **Enter** key, then retype the password to confirm it. At this point, the dsinstall utility tries to create the SCALE tree. If the operation is successful, dsinstall displays the message:

```
DSInstall will now try to acquire a SCALE License... Please wait.

SCALE License successfully acquired.

Number of volumes installed into the Directory: 1 (DSINSTALL-4.2-139)

Installation of Directory Services on this server successful. (DSINSTALL-4.2-26)


Press Enter to continue.
```

4. We recommend that you record the information (tree, context and password) supplied during configuration. You need the information the first time you log in to the server as user ADMIN.

Note

If the dsinstall utility cannot find a SCALE license certificate, the installation fails. Make sure the iFOR/LS license system has a valid SCALE license certificate for the server.

5.4.6 Accessing NNS over a Router

An NNS server can easily be accessed through a router. To do this, however, the router must be running the SPX/IPX protocol and be configured to talk over both adapters in the system. One advantage that SPX/IPX has over NetBIOS is that it can also pass server names through the router automatically (clients can see server names).

In our network, we have a client that communicates to our local network via a router, an RS/6000 called lv3010b. Our local network, where the NNS server resides, is configured on a token-ring and the client network is configured on ethernet.

To enable the client to talk to the NNS server, we have to configure SPX/IPX on the router. For our network we decided to use the version of SPX/IPX that is provided with AIX Connections.

After AIX Connections has been installed we can configure SPX/IPX for both Ethernet and token-ring adapters. The simplest way to configure SPX/IPX with AIX Connections is to use the Quick Start menu from SMIT. We can use this to configure the internal and token-ring interfaces:

1. On the router, from the command line enter:

   ```
   smit aconn
   ```

2. Select **Quick Start**.
3. Select **NW**.
4. Select **/dev/dlpi/tr:0**.
5. A panel will appear (see Figure 61). Enter the network number. In our example the NNS server uses 0x7007.
6. Select the frame type. Our NNS server uses token ring.

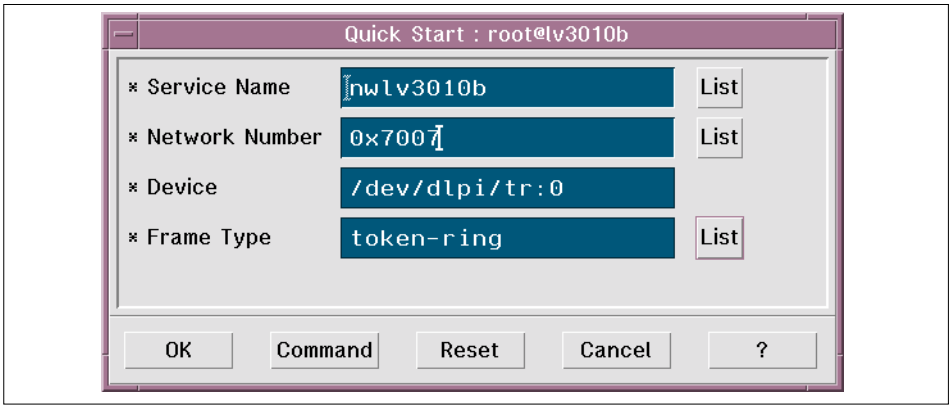


Figure 61. NW Quick Start SMIT Panel

7. Click on **OK**.

After clicking on OK, AIX Connections will start a service for NetWare. We do not need this, so we can stop it. Since we are going to configure another interface we need to stop the IPX daemon as well:

```
/etc/rc.nwserver stop
/usr/tn/IPXd -k
```

We can now configure the Ethernet adapter. We are using en0 for our Ethernet interface which means that we must use a frame type of ethernet_ii:

1. On the router, from the command line enter:

   ```
   smit ipxface
   ```

2. Enter **en0**.
3. Select **/dev/dlpi/en:0**.
4. A panel appears (see Figure 62 on page 117).

5. Select Network Number: **100**.
6. Select frame type: **ethernet_ii**.

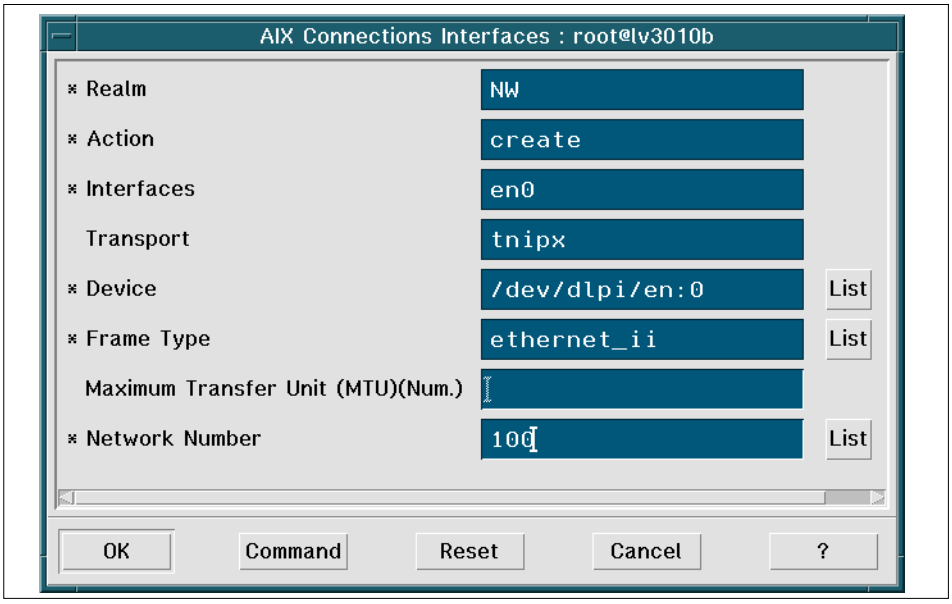


Figure 62. SMIT Panel to Configure Second IPX Interface

7. Click on **OK**.

SPX/IPX is now configured to use both adapters. To start the IPX daemon, simply type:

```
/usr/tn/IPXd
```

This will start SPX/IPX. You can remove the /etc/rc.nwserver line from the inittab and substitute it with a line to start the IPX daemon so it will start automatically during reboot, but not start the NetWare service.

You can check that the SPX/IPX daemon is receiving and sending packets through the different interfaces with the `tnistat` command:

```
# /usr/tn/NW/tnistat
Name          Address                Ipkts   Ierr Opkts  Oerr
en:0          00000100:08005af8d6cc  211     0    105    0
tr:0          00007007:0004ac6173ee  417     0    17     0
internal      090301a3:00007fffffff  0       0    0      0
```

5.4.7 Start, Stop and Check NNS for AIX

The following is the procedure to start NNS. At the AIX command line type:

1. `smitty ncps`

The following panel appears:

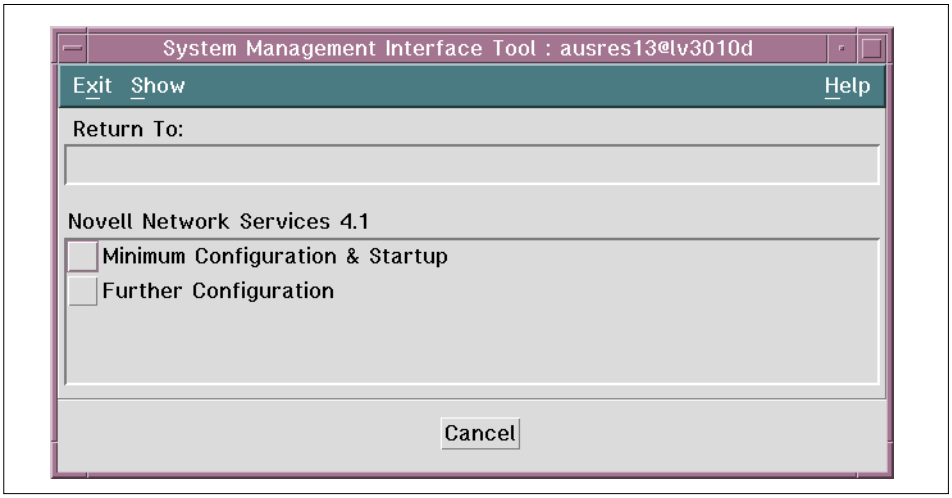


Figure 63. Output of the Command smit ncps

2. Select **Further Configuration** -> **Start the NetWare Server**. This option starts all the NetWare server daemons, the NDS daemons, the printer server and the IPX/SPX protocol. The following panel is displayed:

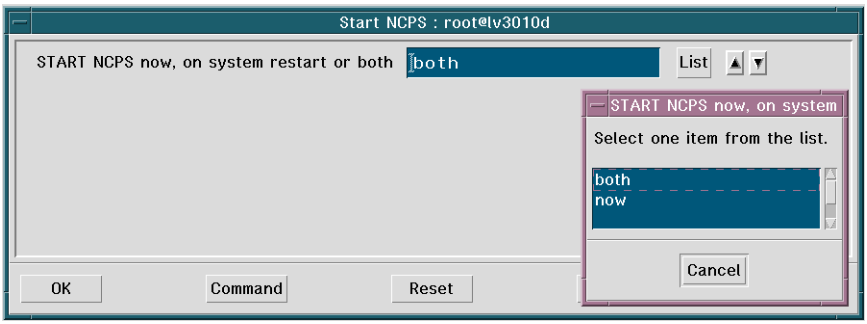


Figure 64. Start ncps

At this time, we have the option of starting the server processes at system reboot time, now, or at both times. If we choose `both` or `restart`, an entry is added to the /etc/inittab file for the server. The entry is:

```
ncps:2:wait:/usr/bin/nw start > /dev/console 2>&1
```

To start the NetWare server from the command line, type:

```
nw start
```

3. If we want to check the server status, we select **Further Configuration** -> **Display Server Status.** A message about server status is displayed, indicating that the server is up, down or coming up. We have to wait until the display confirms that the server is up before trying to connect to the NetWare server. To check server status from the command line, type:

   ```
   nwserverstatus
   ```

4. If we want to stop the server, we select **Further Configuration** -> **Stop the NetWare Server**. To stop the NetWare server from the command line, type:

   ```
   nw stop
   ```

5.5 NetWare Volumes in the AIX File System

NNS enhances the AIX file systems so they can look and behave like NetWare file systems. NNS volumes appear as if they are NetWare volumes on a native NetWare server. AIX is a hierarchical file system, where the top of the tree called the root node and labeled /. A partition is mounted at a particular AIX directory at or below the root and it appears as a directory to the users. NetWare uses a hierarchical file system, with multiple root nodes called volumes. Each volume has its own tree structure, and users must switch volumes to access another volume's resources. Figure 65 illustrates the differences between these two kind of file systems.

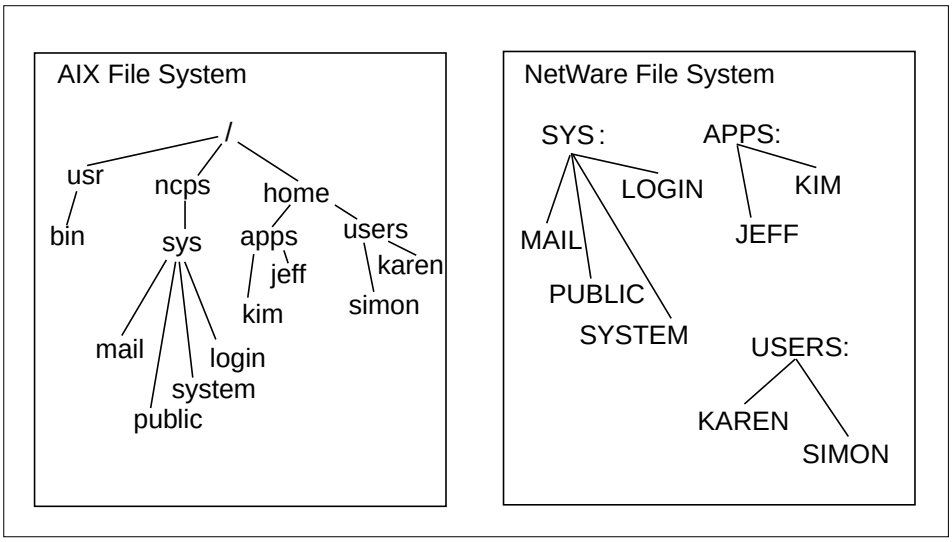


Figure 65. AIX and NetWare File Systems

NetWare volumes on an NNS server are created from the AIX file systems. The SYS volume is created during NNS installation. All other volumes can be created when the NNS server is down and AIX is running. NNS volumes are paths to a particular point in the AIX file system. In Figure 65, the /ncps/sys, /home/apps and /home/users directories become NetWare volumes by specifying these paths in the NNS volume configuration (see 5.5.1, "Volume Configuration Files" on page 121 for details). Windows NT clients, have access to all the files and directories contained within these volumes.

Note

All the AIX directories that are outside a NetWare volume are hidden from NetWare clients and cannot be accessed by them.

NNS volumes are paths into the AIX file system and they do not exclusively own disk space. They depend on the AIX file system for their disk space. There is a deep interaction between the AIX system and NNS volumes. In the next section we speak about this interaction.

5.5.1 Volume Configuration Files

In NNS, all AIX file system information is kept and maintained by the AIX operating system. Since AIX has no knowledge of the type of information required by a NetWare file system, NetWare file system information cannot be kept with the AIX file system information. NNS keeps and maintains NetWare file system information in configuration and control files. When we create a volume with the SMIT panel (see Section 5.7.2 for details), the voltab file in the /etc/ncps/netware directory is upgraded. This file specifies the following:

- Name spaces. UNIX and DOS are always supported; OS/2 is configurable. Windows NT and Window 95 use the OS/2 name space.
- The path into the AIX file system where the NetWare volume should begin.
- The AIX directory path for a control directory.
- Synchronization parameters.
- Access control mode.

The control directory for a NetWare volume must be an AIX directory path that is outside of the NetWare volume. This path specifies the location of the three types of control files that store the NetWare information. The default location for the control directories is /etc/ncps/control. Under the control directory, each volume has a subdirectory named as the volume. For example, the control directory for the SYS volume has the following path: /etc/ncps/control/sys. There are four files stored in the control directory:

- usinodes. It maintains DOS and UNIX names for all the files and directories in the volume. It maintains name space according to the volume's configuration. It also keeps the NetWare file system information (data and time of creation, modification, backup and access). It maintains the NetWare attributes assigned to files and directories.
- trustee.sys. It maintains the trustee assignments granted to the directories and files in the volume.

- extendedNames. It maintains the names for any file or directory that has an extremely long name. Both AIX and Windows NT allow for names to be over 250 character long. Up to 25 character names fit into the usinodes files, but the longer ones are stored in this file.
- LastMountLog. It records any error or consistency failures that occurred the last time the volume was mounted.

These files contain vital information for the NetWare volumes and NNS protects them from the NetWare users by hiding them; they must be outside the NetWare volume. NNS protects them from the AIX users by assigning root as the owner of the files.

5.5.2 Synchronization Requirements

The NetWare file usinode (see Section 5.5.1 for details) requires synchronization with the AIX operating system. AIX users can modify the files and directories in the NNS volume without notifying NNS that something has been changed. NNS sets mandatory synchronization at specified intervals although the NetWare system administrator can change this interval using the SMIT panel (smit ncps-> Further Configuration-> NetWare Volume Manager-> Change/Show a NetWare Volume). Normally, volumes that are accessed only by NetWare users or read-only volumes, require infrequent synchronization. In the first case, NetWare users are responsible for all the file system changes and in the second case no one can make any changes. Volumes that are accessed by both NetWare users and AIX users require frequent synchronization. Since AIX users log in to the AIX operating system and not in to the NetWare operating system, they and their actions are hidden from the NNS server. NNS has to synchronize what it has in the usinodes file with what is currently in the AIX operating system. NNS provides configuration parameters that allow the system administrator to determine the frequency of mandatory synchronization. The default values prevent a volume from being synchronized every few seconds or less than four times an hour.

5.5.3 Validation Process

Volumes are part of the AIX file system and most of the maintenance for file system repair is done by the host operating system. The only exception is the usinodes file. This file is validated every time the NNS server mounts the volume. The validation process writes the inconsistencies to the Last MountLog file.

5.5.4 Moving NetWare Files

AIX administrators have access to the files in NNS volumes. They can copy or move NetWare files from one volume to another with AIX commands, but the AIX commands do not transfer the NetWare file system information with the files. To transfer the NetWare file system information with the file, you have to use the NetWare `NCOPY` or `FILER` commands. These commands are available from a Windows NT-installed client in the folder public in the volume SYS (see Section 5.8.2 for details). These commands only work if you are copying or moving a file from one NNS volume to another. When a NNS volume is moved from one location in the AIX file system to another, it is best to create the second location as a NetWare volume and then use `NCOPY` or `FILER` to move the files. If you are moving a file from an AIX directory to a NetWare volume or from a NetWare volume to an AIX directory, AIX commands must be used.

5.6 File Sharing Services

NNS offers a variety of services that manage access and make files shareable to multiple clients. In the following sections we discuss some of these services.

5.6.1 File Open Modes

By default, NNS flags files Read Write (Rw) when they are created. This attribute ensures that the file can be accessed and opened by only one user. NNS also has Read-Only attribute (Ro) and a Shareable attribute (Sh). NNS uses the Rw, Ro and Sh attributes to determine how to open a file. Files with the Rw attribute are opened in a mode that denies other users access to the file. Files with the RoSh attributes are opened in a mode that allows other users to open the file in a read-only mode but denies access to those users who want to open the file for writing. For example, all the NetWare utilities in the public folder in the SYS volume are flagged RoSh so they are accessible to multiple users at the same time. Since NNS is running on the AIX operating system and it uses the AIX file system to store the file, NNS must issue open calls to the AIX file system to open files for NetWare users. AIX does not use NetWare open modes or attributes for determining who can open the file. AIX uses the file permission granted to the owner, group and others to determine who can open the file. During the NNS installation (see Section 5.4.3) one group, *nwgroup*, is created. Four users belonging to nwgroup have been created: *nwroot*, *nwprint*, *nwldap* and *nwuser.* NNS uses these accounts to assign permissions to the files created by NetWare users. In this way, the NetWare files are protected from AIX users because the NNS users own the files. It is allowed to change this behavior with the NNS hybrid user feature (see Section 5.6.2).

5.6.2 Hybrid User

The hybrid user is the feature that facilitates coordination between a NetWare user account and an AIX user account. On an NNS server, three types of users are possible:

- *NetWare users*. They have a NetWare user account but they do not have an AIX user account.
- *AIX users*. They have an AIX user account but they do not have a NetWare user account.
- *Hybrid users*. These users have NetWare and an AIX user accounts and can access the same files from either account.

Note

Without the hybrid feature, NetWare user accounts are hidden from AIX.

Table 2 and Table 3 illustrate this concept using a simple example.

Table 2. NNS Connection Table

User	Open Files
Kim	filenew.txt
Simon	readme.txt, newconfig

Table 3. AIX Connection Table

User	Open Files
Bob	oldfile.txt
nwroot	readme.txt, newconfig, filenew.txt

This example shows us two NetWare users logged in, both with files opened. The AIX operating system do not recognize these NetWare users. When an NCP engine (see Section 5.2.5) opens a file for a NetWare user, the NCP engine uses its assigned default AIX user ID (UID), nwroot, to open the file. The hybrid user feature allows the system administrator to change the default UID used by the NCP engines when opening and creating files. By default, NetWare users create files owned by nwuser, assigned to nwgroup. NNS assigns a permission mask configurable from the AIX command line with the command `nwcm` (for more information, see the *Novell Network Transport Services 4.1 for AIX Reference* manual, sc23-4135). When the AIX users log in to their AIX user accounts, they cannot access the files that they previously created as NetWare users, because nwuser owns the file. The hybrid feature can map the NetWare account to the AIX account. If this feature is activate on the NNS server, when a NetWare user creates a file, the AIX account of this user will become the owner of the file. Users with both NetWare and AIX accounts can be made hybrids users by associating their AIX login names with their NDS common names (CN) (see Section 5.3.4). To allow the hybrid users to be known to the NNS server, follow these steps:

1. Create the file /etc/ncps/nwusers. An example entry may look like the following, where on the left we have the Typeful NDS names and on the right we have the AIX names.

```
CN=KIM.OU=LAB.O=IBM kim
CN=SIMON.OU=LAB.O=LAB simon
```

Note

If you are using a SANDS server, the entries needs to contain the tree name (in our example: `CN=KIM.OU=LAB.O=IBM T=NDS1 kim`).

2. smit ncps -> **Further Configuration** -> **Hybrid User** and the following panel appears:

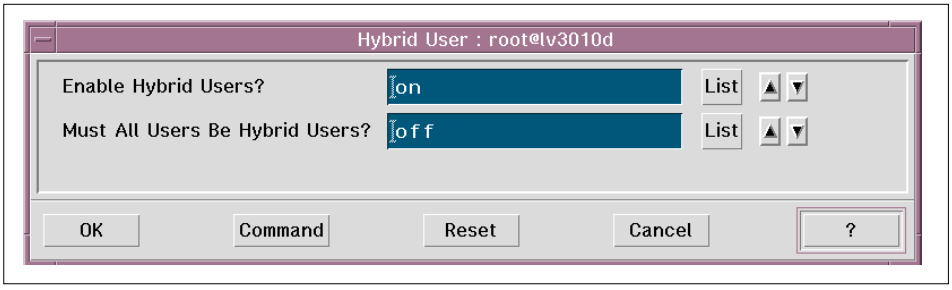


Figure 66. Hybrid Users Panel

3. Enter on in the Enable Hybrid Users? field. The NNS server will check the /etc/ncps/nwusers file when a NetWare user logs in. If an AIX user name has been assigned to the NetWare user, all files and directories created by the NetWare user will be owned by the assigned AIX user. If the field Must All Users Be Hybrid Users? is set to `off`, it means that the NetWare users who do not have a mapping in the /etc/ncps/nwusers file will use the nwuser account. If it is set to on, all NetWare users must have a mapping or they cannot log in.
4. The NNS server must be restarted (see Section 5.4.7). For more information, refer to “Setting Up a Hybrid User” in *Novell Network Services 4.1 for AIX Supervising the Network* (SC23-4140-00).

5.7 Additional NNS Configuration

There are several other configuration elements that you may decide to modify from the default setting to adapt your need.

5.7.1 Setting Bindery Context

When a NNS server is installed into the directory tree, the bindery context is set by default to the container into which the server is installed. To set our bindery context at the AIX command line type:

1. `smit ncps`
2. Select **Further Configuration** -> **NetWare Server** -> **Directory Services** and the following screen appears:

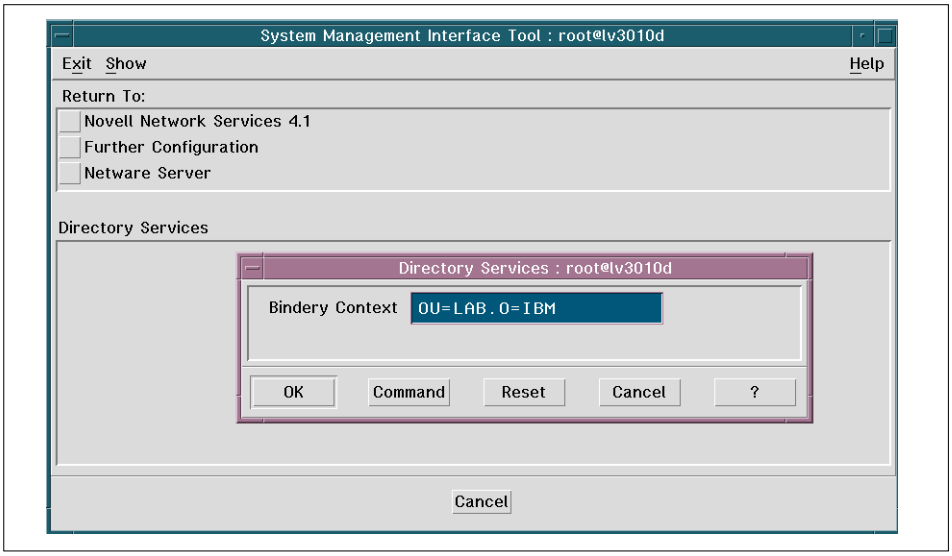


Figure 67. Setting Bindery Context

3. We have to enter our bindery context. This alters the ds_bindery_context variable, which sets the location from which the bindery clients will scan.

5.7.2 Volume Management

Volume is the highest print in a NetWare file system. Volumes contain directories, subdirectories and files. In NNS, each NetWare volume is a path to a point in the AIX file system. The NetWare users cannot see the AIX directory structure above the NetWare volume level. To the AIX administrator,

NetWare volumes appears as AIX subdirectories. The installation process creates a default container object for the volume SYS. The AIX directory for the volume SYS is /ncps/sys.

Note

The NNS server must be stopped before configuring a new volume or making any modifications to existing volumes.

The following is the procedure to create a new volume:

1. At the AIX command line, type `smit ncps`
2. Select **Further Configuration** -> **NetWare Volume Manager** and the following screen appears:

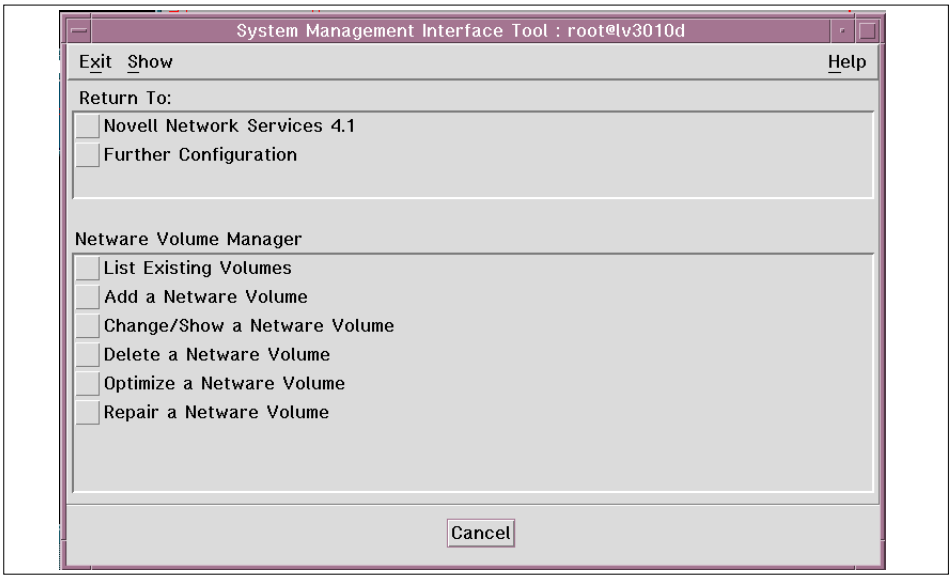


Figure 68. Managing Volumes

Note

NetWare supports a maximum of 64 volumes.

3. From this panel, we can list the existing volumes, add a volume, modify a volume, delete a volume or optimize/repair a volume. To add a new volume, select **Add a NetWare Volume**. The following panel is displayed:

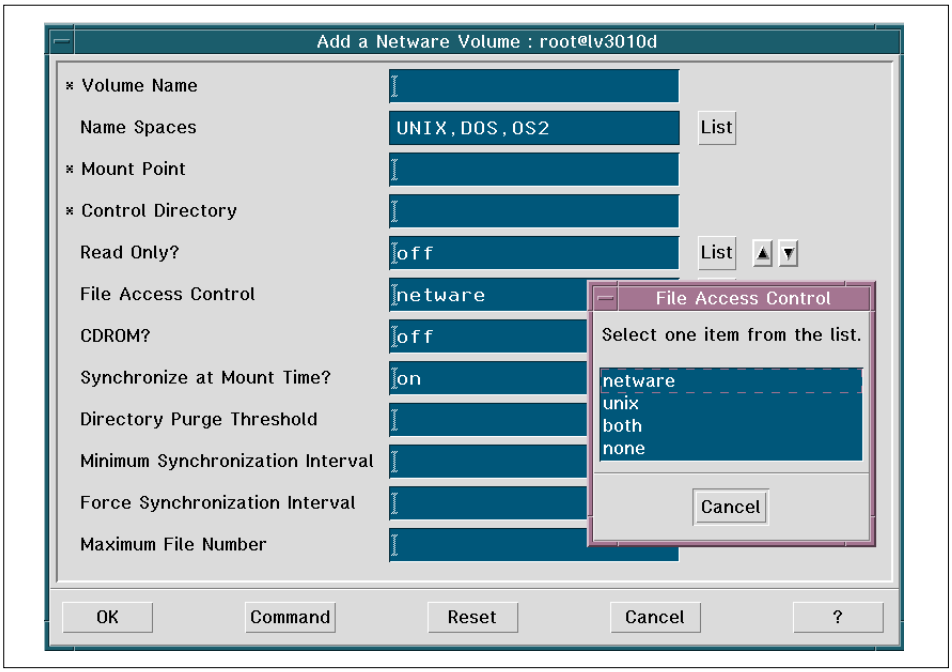


Figure 69. Adding a Volume

Note

The Mount Point of the volume and the Control Directory must be created before a volume is created.

4. Enter the volume name. Volume names are two to 15 characters long. In the Name Space field leave UNIX, DOS, OS2 if you want to manage file names longer than 11 characters (8 for the name 3 for the extension). The mount point specifies the directory where the file system is available or will be made available. The control directory is the directory where NNS volume control information is stored. The control directory for a NetWare

volume must be an AIX directory path that is outside of the NetWare volume. A good naming convention is shown in Table 4.

Table 4. Naming Convention Table

Volume	Mount Point	Control Directory
SYS	/ncps/sys	/etc/ncps/control/sys
USERS	/home/users	/etc/ncps/control/users
APPS	/home/apps	/etc/ncps/control/apps

The File Access Control field specifies the file access mode for NetWare users. It can be **netware** (trustee assignments control a NetWare user's access), **UNIX** (AIX permissions control a NetWare user's access), **both** (both NetWare trustee assignments and AIX permission control access), or **none** (all NetWare users can access the files and directories as if they had supervisor rights).

5. We must now start the NNS server before upgrading the NDS database.
6. The next step is to add the NDS volume object into the NDS database. At the AIX command line, type:

- `smit ncps`
- Select **Further Configuration** -> **Configure Network Directory Services using dsinstall**. The following screen appears:

```
        1) Install a new SANDS tree
        2) Install a new SCALE tree
        3) Add a new server into an existing SCALE tree
        4) Upgrade this SANDS server/tree to SCALE
        5) Remove Directory Services from this server
        6) Upgrade mounted volumes into the Directory
        7) Exit

Enter option number:
```

- Select option 6, **Upgrade mounted volumes into the Directory**. Input the NDS tree name, organization, and ADMIN password. When the required information is entered, dsinstall tries to log in to the NDS tree. If login succeeds, the dsinstall utility upgrades the newly-added server volumes into the NDS database. The panel looks like the following:

```
       1) Install a new SANDS tree
       2) Install a new SCALE tree
       3) Add a new server into an existing SCALE tree
       4) Upgrade this SANDS server/tree to SCALE
       5) Remove Directory Services from this server
       6) Upgrade mounted volumes into the Directory
       7) Exit

Enter option number: 6

Enter the NDS Tree Name: NDS1

Enter the ADMIN user context (e.g. OU=aa.OU=bb.O=cc): OU=LAB.O=IBM

Enter the ADMIN password:

Logging into the tree... Please wait.

Number of volumes installed into the Directory: 1 (DSINSTALL-4.2-139)


Press Enter to continue.
```

7. To list the existing volumes, type:

- `smit ncps`

- Select **Further Configuration** -> **NetWare Volume Manager -> List Existing Volumes.** The following screen is displayed:

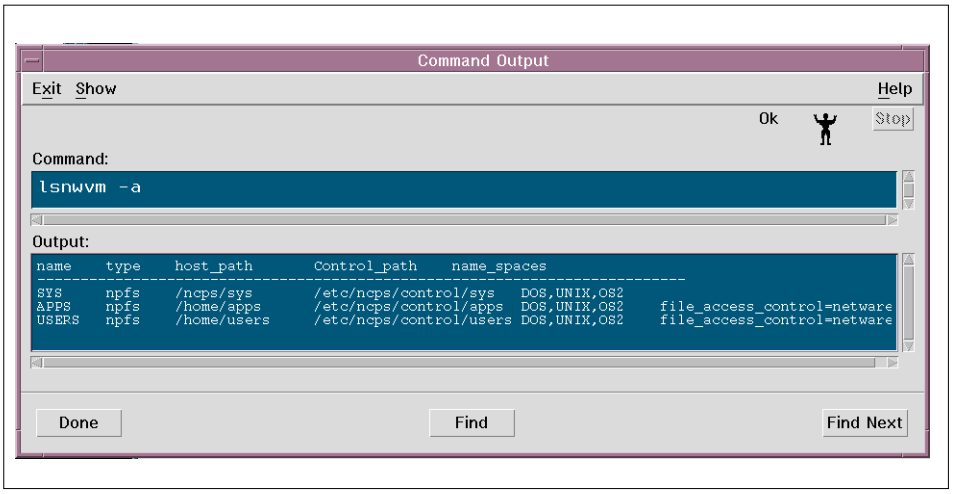


Figure 70. Listing Existing Volumes

5.7.3 Adding Additional Objects

The installation process creates a default container object for the volume SYS. In the previous section we discussed adding additional volumes. In the installation process, another object, called ADMIN, is created and placed at the top of the directory tree. Before we can continue setting up our network, we must install a single client. From the client, we can run either NetWare Administrator (NWADMIN) or NETADMIN to start creating objects on our network. From the RS/6000 running NNS Server we cannot create and manage objects. The SMIT panels available do not allow you to execute these tasks. For more information, see sections 5.8, “Clients Installation” on page 139 and 5.10, “Client Operations” on page 165.

5.7.4 LDAP Services

Lightweight Directory Access Protocol (LDAP) is a scaled-down version of the X.500 Directory Access Protocol (DAP). This protocol is becoming the standard access protocol for Internet and intranet clients browsing for directory information. LDAP Services for NDS allows you to configure NDS to publish public and/or private information that companies want to share with the world. NNS’s implementation of the Lightweight Directory Access Protocol (LDAP) requires the following software modules:

- Server Module running on RS/6000: nwslap daemon

- LDAP Administrative module running on Windows NT or Windows 95 workstations
- LDAP-compliant Internet browser or application

The NDS information that is most commonly available through LDAP are user name, e-mail addresses, work phone numbers and fax numbers. LDAP services for NDS uses both NDS security and LDAP security to control the clients that can access NDS and the information the clients can access and modify. LDAP requires the following steps to make NDS information available to a LDAP browser:

- Enter the information into the NDS database.
- To access the NDS database information, LDAP clients must be given NDS and LDAP rights.

5.7.4.1 Installing LDAP on the Windows NT Client

From a Windows NT client installed with the administrative capability, follow this procedure:

1. Map a drive from the NNS server where the LDAP services will be available (see Section 5.10.1, “How to Map a Drive” on page 165 for details).
2. Create a LDAP installation directory.
3. Copy the LDAP software (ldap_v1.exe) from the /ncps/sys/public/ldap directory on the NNS server to the installation directory. Run the **LDAP_V1.EXE** program to extract the files. The installation directory is shown in Figure 71.

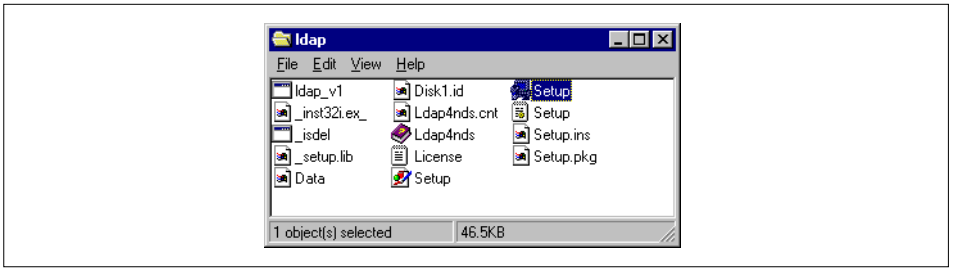


Figure 71. Ldap Installation Directory

4. From the LDAP installation directory, run the **SETUP.EXE** program and the following window appears:

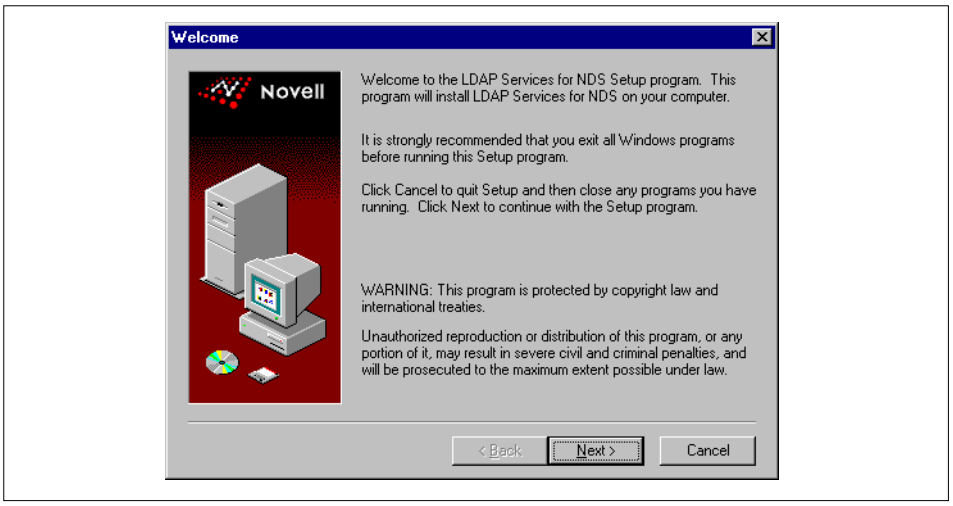


Figure 72. LDAP Installation

5. Select **Next** to display the software license agreement. In the following panel select **Yes** to display the Setup Options panel (Figure 73).

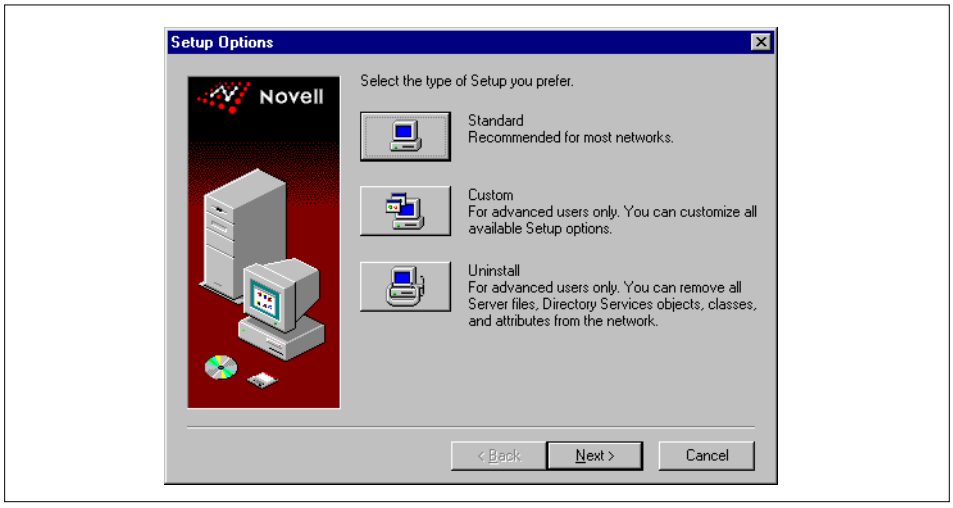


Figure 73. Setup Options Panel

6. Select **Standard**, then select **Next** to install all LDAP Service software.
7. When the Select Administration Files Destination Directory appears, select the directory in which the NetWare Administrator snap-in utility will

be stored and then select **Next.** If the message in Figure 74 appears it means that you do not have a mapped drive.

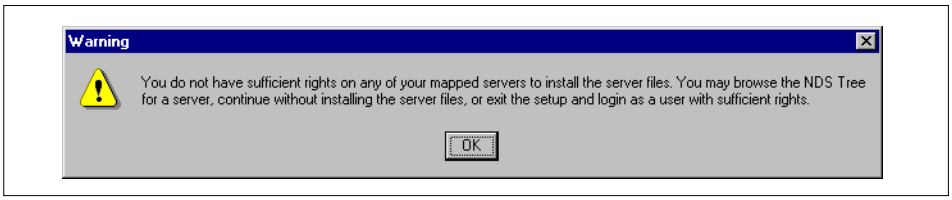


Figure 74. Error Message

8. When the Select Destination Server from those with Mapped Drives panel appears, select the NNS server on which you want to install LDAP services, and then select **Next** (Figure 75).

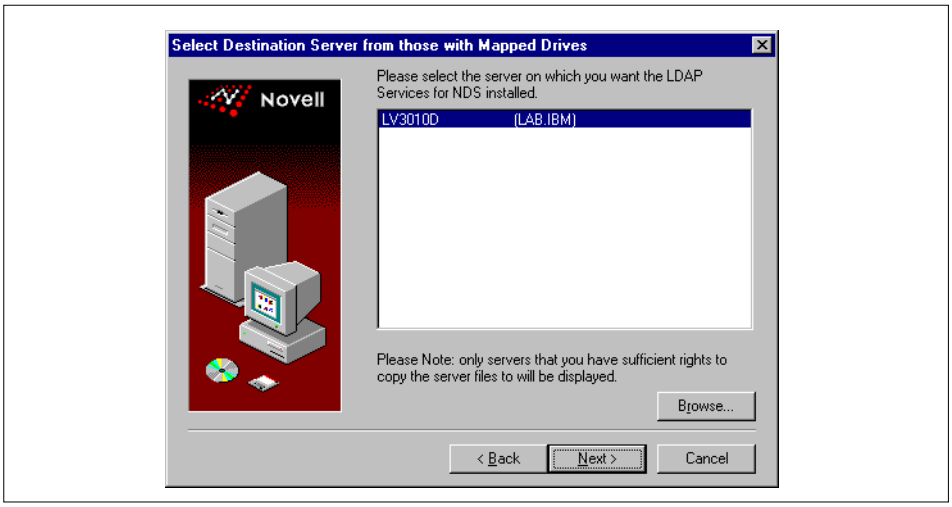


Figure 75. Select Destination Server from Those with Mapped Drives

9. Figure 76 shows the Installation Information panel. Verify that the selections are correct, and then select **Next**.

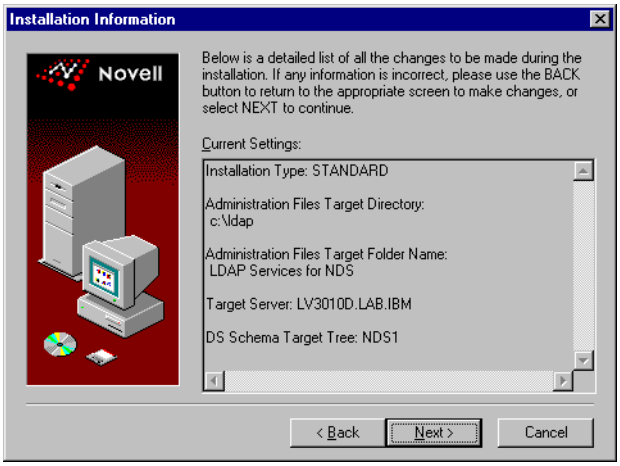


Figure 76. Installation Information

10. For information about customizing access and security, use the online help, **Ldap4nds**, installed in the LDAP directory.

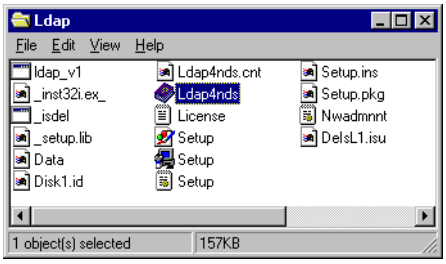


Figure 77. Ldap Folder

5.7.4.2 Configuring and Starting the LDAP Daemon

During the installation, NNS creates the user nwldap (see Section 5.4.3). The LDAP daemon uses the nwldap user. To configure and start LDAP services, follow these steps:

1. Configure the NetWare UnixClient (NUC) for LDAP. To do this at the AIX command line, type:

   ```
   smit ncps
   ```

2. Select **Further Configuration** -> **LDAP Configuration & Startup** and the following panel appears:

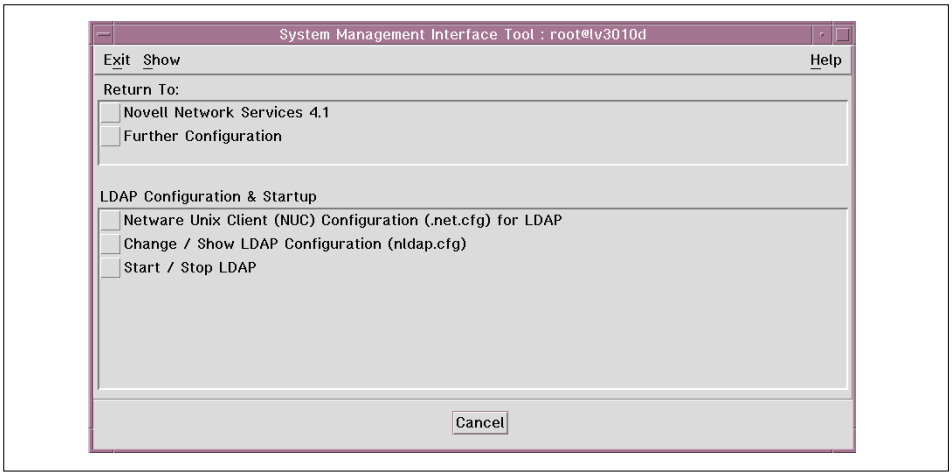


Figure 78. Configuring NUC

3. Select **NetWare Unix Client (NUC) Configuration (.net.cfg) for LDAP**. The following panel appears:

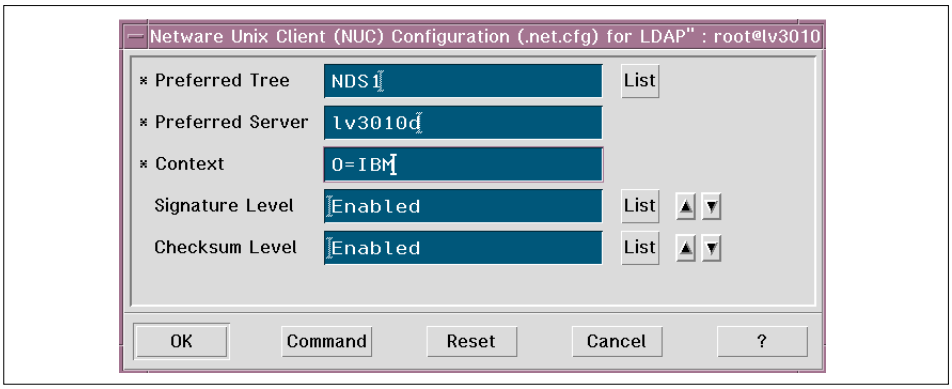


Figure 79. Configuring NUC

4. Enter the Preferred Tree name, the Preferred Server name and the Context. The context must have the `O=` designation.
5. To configure the LDAP daemon at the AIX command line, type:

   ```
   smit ncps
   ```

6. Select **Further Configuration** -> **LDAP Configuration & Startup** -> **Change/Show LDAP Configuration (nldap.cfg)** and the following window appears:

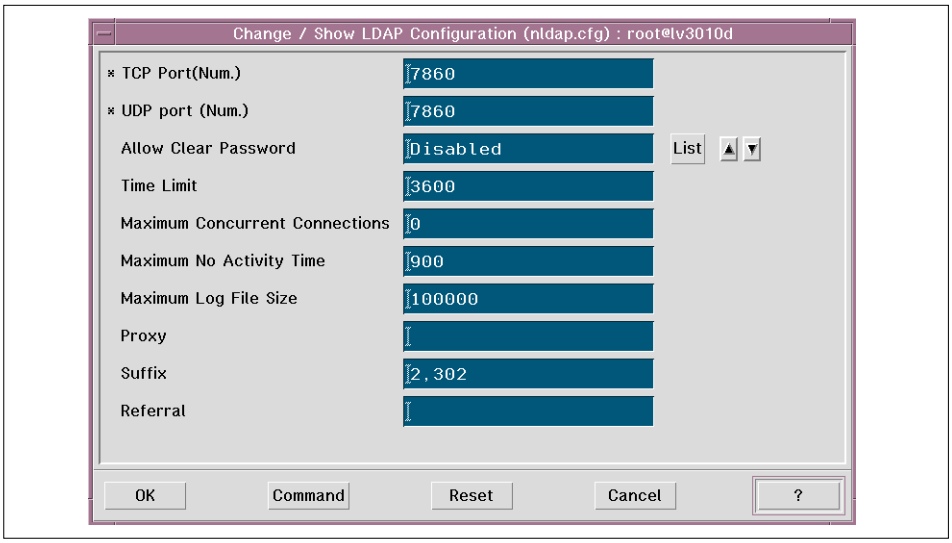


Figure 80. Change/Show LDAP Configuration

7. Check the TCP and UDP port number. Change the default value if another process is using it. Other fields can be left at the default values. Press the **Enter** key to save the changes.
8. Start the LDAP daemons. At the AIX command line, type:

   ```
   smit ncps
   ```

9. Select **Further Configuration** -> **LDAP Configuration & Startup** -> **Start/Stop LDAP**. The following window appears:

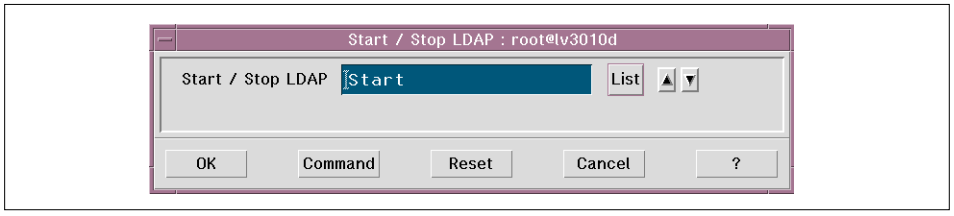


Figure 81. Start/Stop LDAP Daemon

10. Press the **Enter** key to start the LDAP daemon. After configuration, the LDAP daemon will be started automatically at the NNS server restart.
11. Once the LDAP daemon is up and running, you are ready to log in from a Windows NT workstation running LDAP client software.

Note

For detailed information on customizing access and security, use the online help application that comes with the NetWare administrator snap and the Ldap4nds book in the LDAP installation directory on the Windows NT client.

5.8 Clients Installation

In this section we discuss two types of clients:

- WIN-NT 4.0 NetWare Client and Gateway
- Novell internetwork Client 4.11a for Windows NT

Note

We have to install NWLink IPX/SPX Compatible Transport on our PC client.

5.8.1 Installation of WIN-NT 4.0 NetWare Client and Gateway

Windows NT includes a NetWare client. If Windows NT is installed with a Server license we can see the NetWare Client and Gateway. If Windows NT is installed with a Workstation license, we can only see NetWare Client. This service enables the computer to log on to NetWare servers, access their resources, and manage administrative tasks. Perform the following steps to install this service:

1. Open the **Network** item in the control panel and select **Services**. The following window appears:

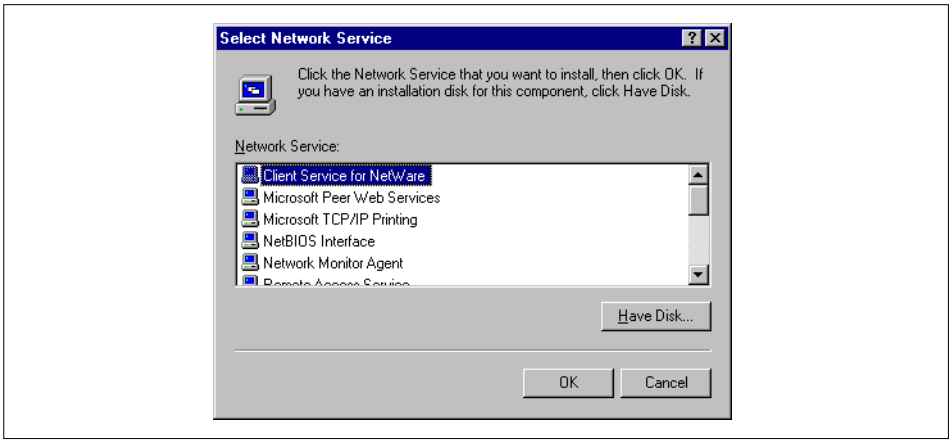


Figure 82. Network Services Window

2. Select **Client Services for NetWare** and then click on **Add**.
3. At the end of the installation we must shut down and restart our PC before the new settings will take effect.
4. To check that both installations (Client Services for NetWare on PC computers and the previously-installed NNS server on RS/6000) were successful from the Windows NT desktop, click on the **Network Neighborhood** icon. The following window appears:

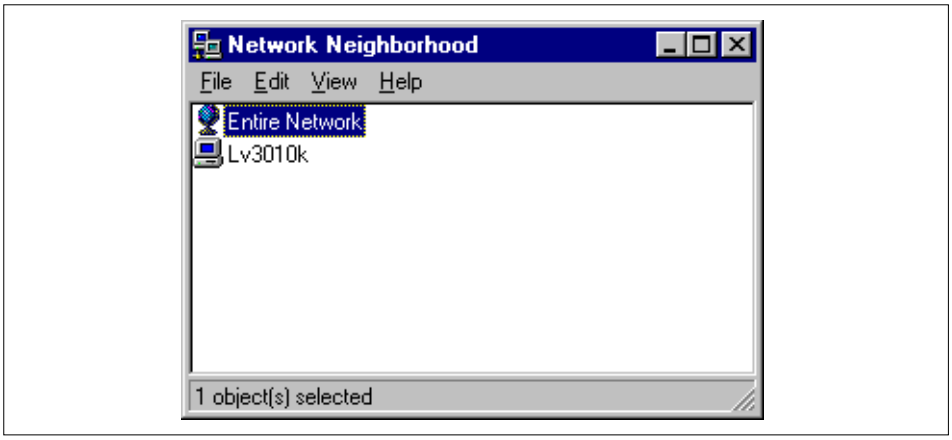


Figure 83. Network Neighborhood Window

5. First click on **Entire Network**. A window will appear (as shown in Figure 84). Then click on **NetWare Compatible Network**.

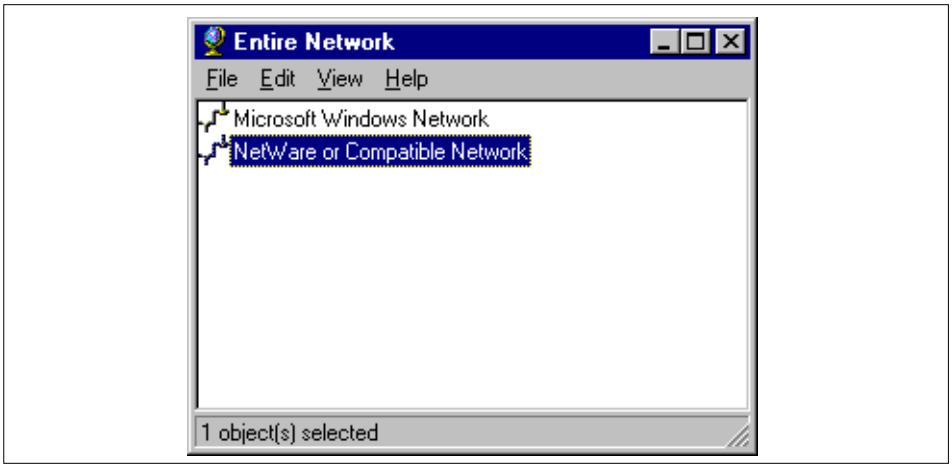


Figure 84. Entire Network Window

6. Having clicked on the NetWare Compatible Network, another window will appear (as shown in Figure 85). In this window we can see our NNS server (in our example, lv3010d).

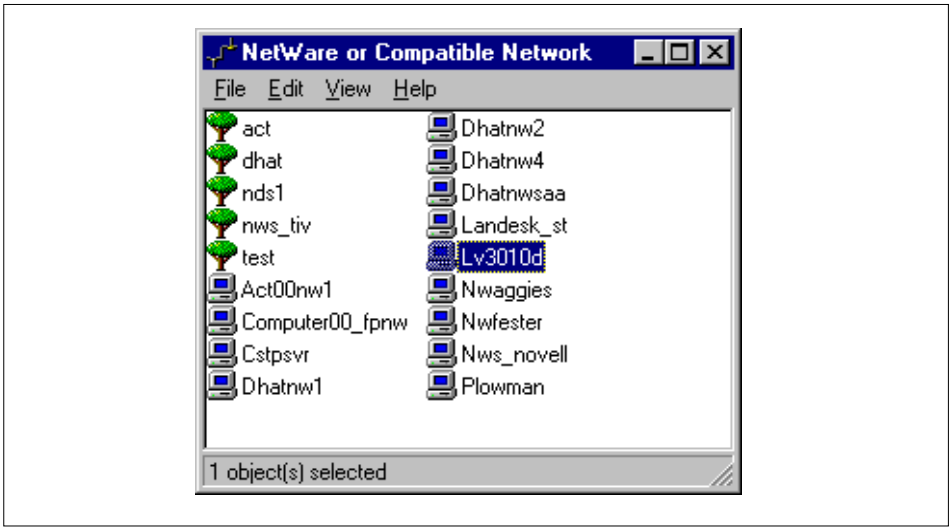


Figure 85. NetWare or Compatible Network Window

7. If we click on the **lv3010d** system in the window, we will be presented with a dialog box as shown in Figure 73. Since we have set a default account during the NNS installation on the server (user ID admin password admin), we can log in to the NNS server.

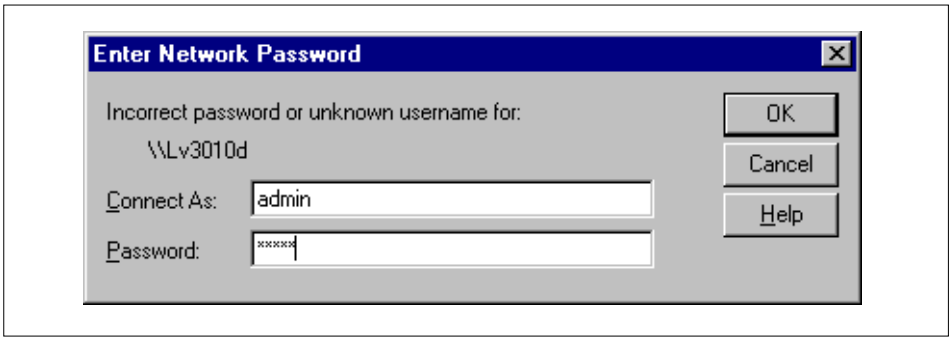


Figure 86. Enter Network Password Window

8. Having logged on to the NNS server, we can now access the resources that are available. Figure 87 shows the resources that are available on lv3010d. They are a list of available volumes on the NNS server.

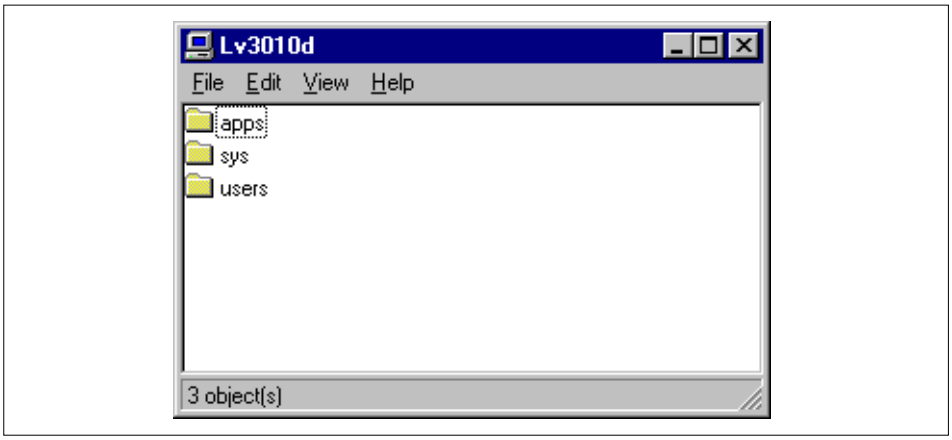


Figure 87. NNS Resources Window

9. If we click on one of these volumes, in this example sys volume, we can see the contents as shown in Figure 87.

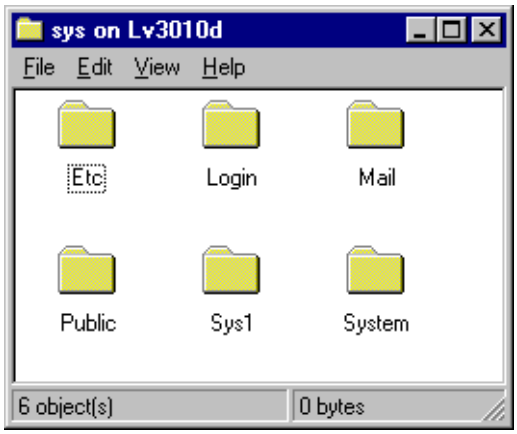


Figure 88. sys Contents Window

10. If we click on the **Public** folder in the window, we are presented a list of directories and files, as shown in Figure 89.

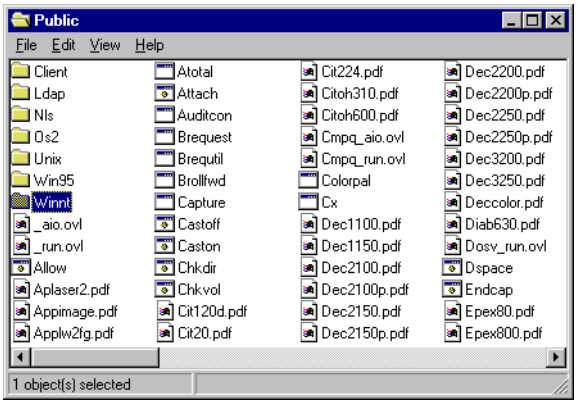


Figure 89. Public Contents Window

11. Now click in the **Winnt** folder that contains the Adm411nt program, as shown in Figure 90. This program is the NetWare Administrator for Windows NT.

Figure 90. Winnt Folder Window

12. We need at least one client installed with the NetWare Administrator for Windows NT. This allows us to manage administrative tasks. To install this program, click on the **Adm411nt** icon and, after a message appears asking for our confirmation to install, the following screen appears:

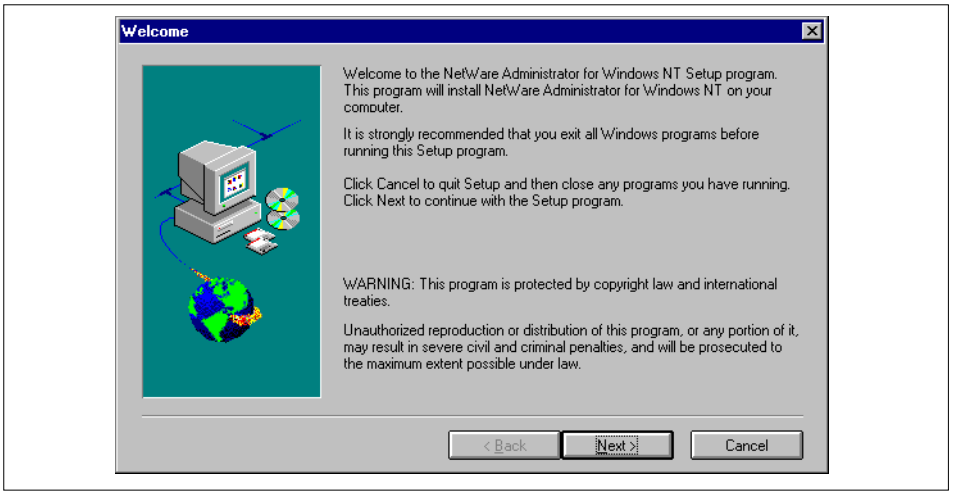


Figure 91. Welcome to the NetWare Administrator for Windows NT Window

13. Now we have to follow the steps required by the installation program.

5.8.2 Installing Novell intranetWare Client 4.11a on Windows NT 4.0

This is the Novell client available on the Web. This release supports the following platforms:

- Intel-based Windows NT Workstation 3.51 workstations, with Service Pack 4 installed
- Intel-based Windows NT Workstation 4.0 workstations

We have to download the code from the Novell Web site: `www.novell.com`. In the NetWare/intranetWare section there is the software intraNetWare Client 4.11a for Windows NT. There are three files named ennt4111.exe, ent4112.exe, and ent4113.exe. We can download these files to a directory on our PC (Figure 92), and then begin the installation as described in the following steps.

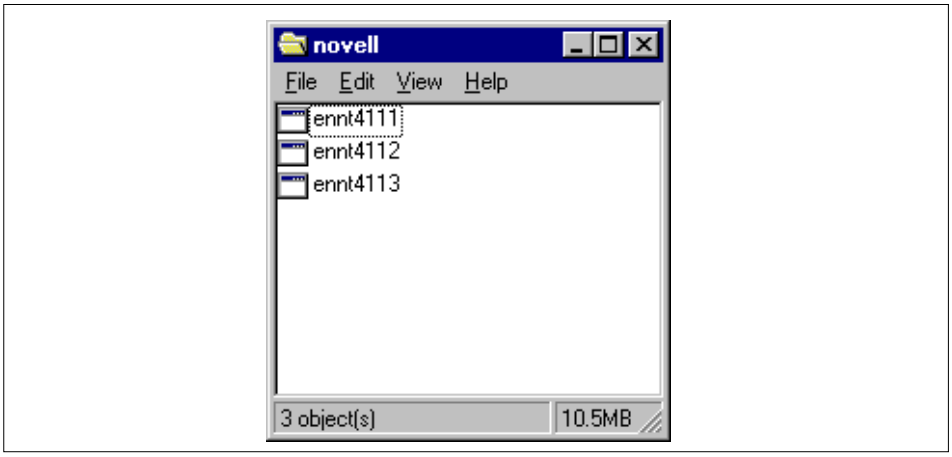


Figure 92. Novell intraNetWare Client 4.11a for Windows NT Executable

1. Click on the **ennt4111** icon and wait for the end of the task. Do the same for **ennt4112** and **ennt4113**. After completing these tasks, we have to run the setup configuration program from the **I386** folder created from the installation procedure. The folder's contents are shown below:

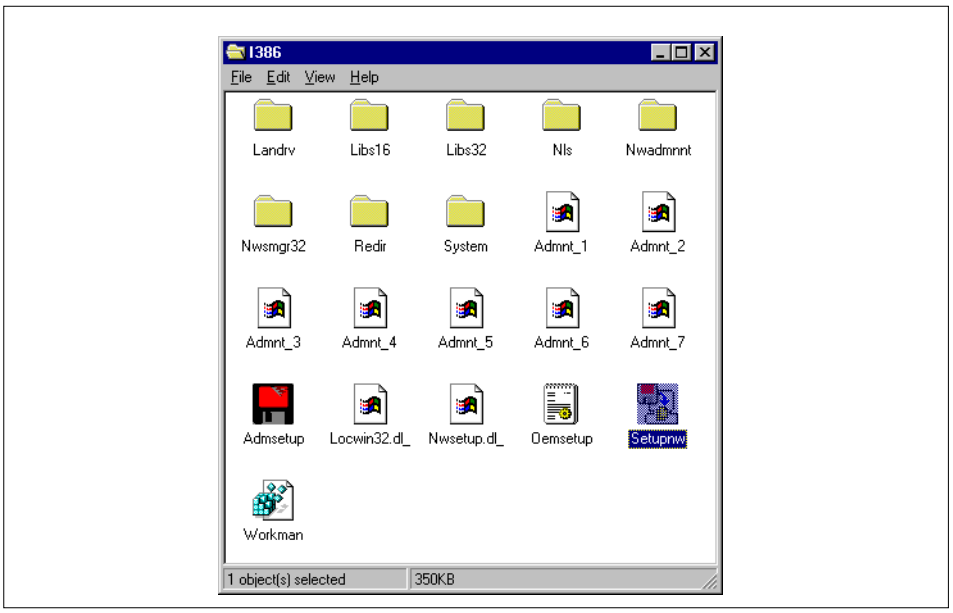


Figure 93. I386 Folder Contents

2. Click on the **Setupnw** icon and a message will appear (Figure 94). To continue the install process, press **Continue**.

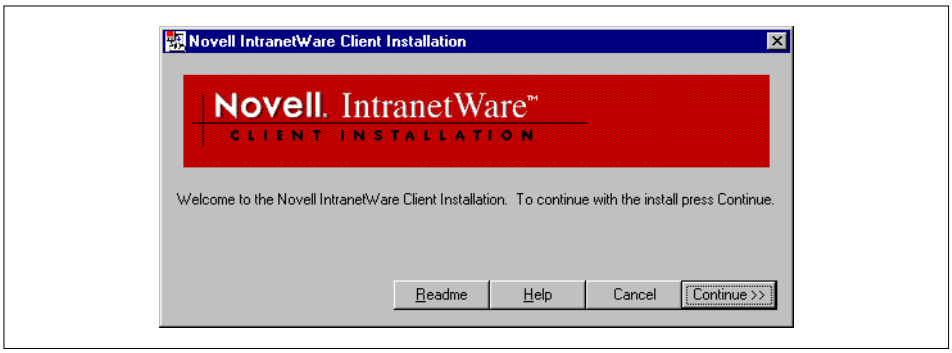


Figure 94. Novell intraNetWare Client Installation Window

3. To check that both installations (Novell intraNetWare Client on the PC and the previously-installed NNS server on the RS/6000) were successful from the Windows NT desktop, click on the **Network Neighborhood** icon. The following window appears:

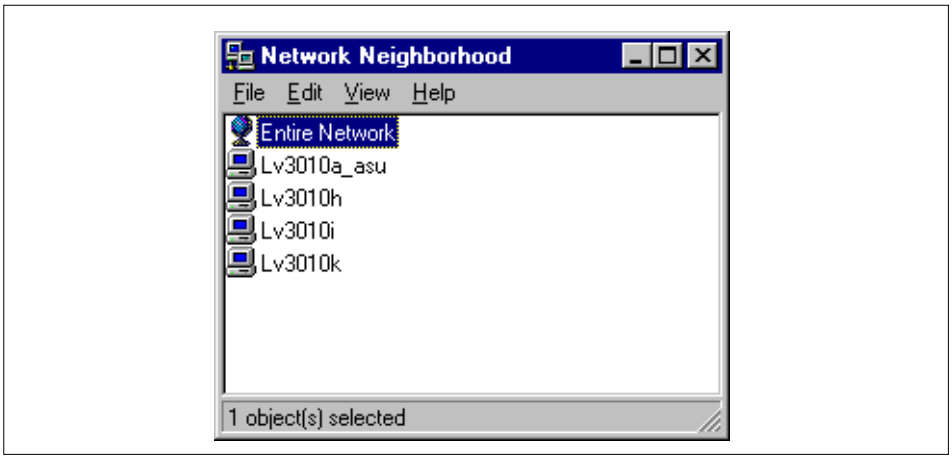


Figure 95. Network Neighborhood Window

4. Click on **Entire Network** and a window appears. Then click on **NetWare Services**.

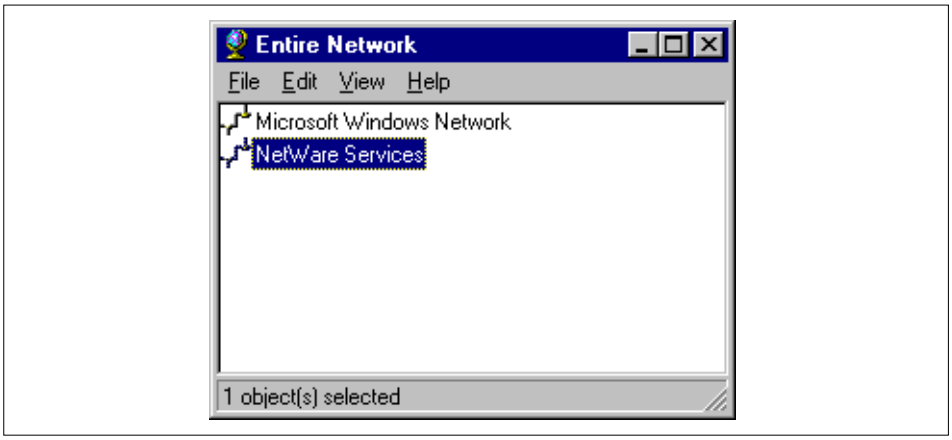


Figure 96. Entire Network Window

5. Having clicked on the NetWare Services, another window appears (as shown in Figure 97). In this window we can see both intraNetWare Servers and Novell Directory Services.

Figure 97. NetWare Services Windows

6. Click on the **IntraNetWare Services** icon. In the following window we can see our NNS server (in our example, lv3010d).

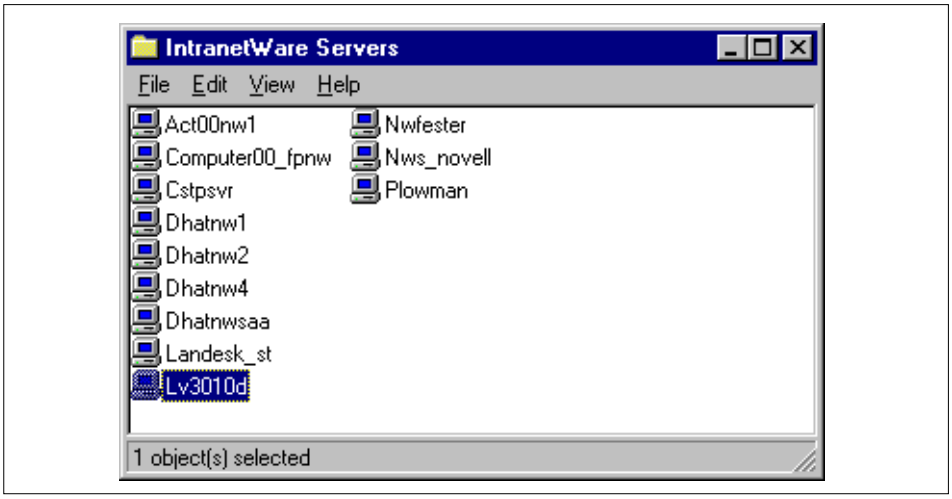


Figure 98. IntranetWare Servers Windows

7. If we click on the **lv3010d** system in the window, we are presented with a dialog box as shown in Figure 99. Since we have set a default account during NNS installation on the server (see Section 5.4.5), we can log in to the NNS server. The user ID and password is `admin`.

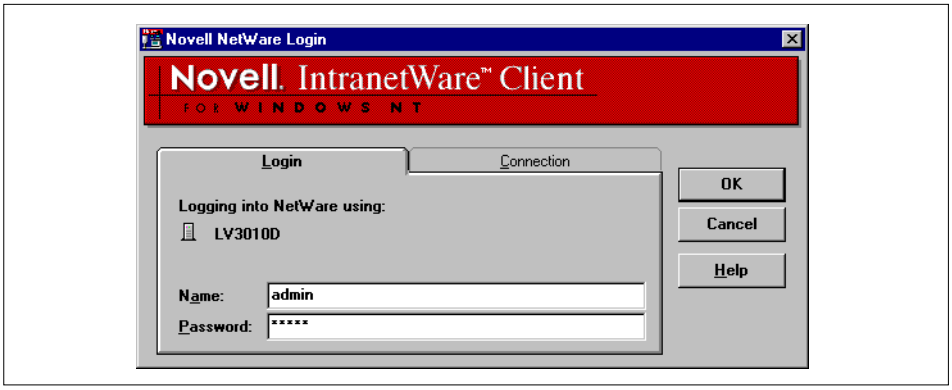


Figure 99. Novell IntranetWare Password Window

8. Having logged on to the NNS server, we can now access the resources that are available. Figure 100 shows the resources that are available on lv3010d. They are shown as a list of available volumes on the NNS server.

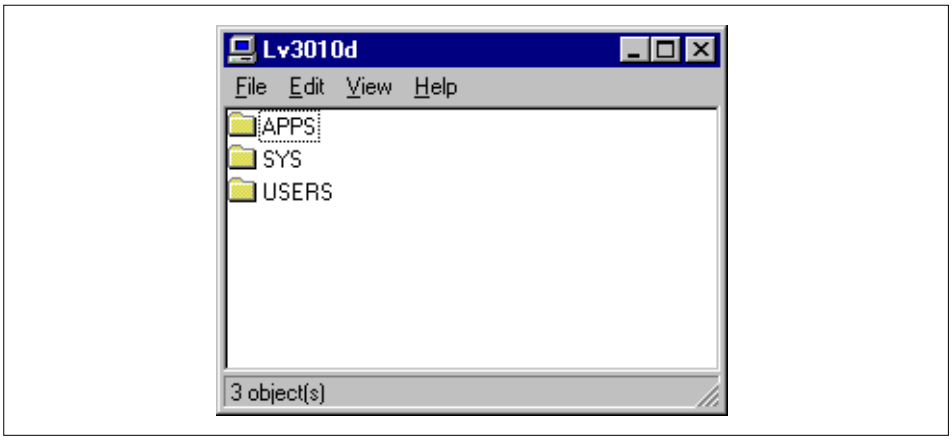


Figure 100. NNS Resources Window

9. We need at least one client installed with the Novell intraNetWare Administrator for Windows NT. This allows us to manage administrative tasks. To install this program we have to click on the **I386** icon and the following screen appears:

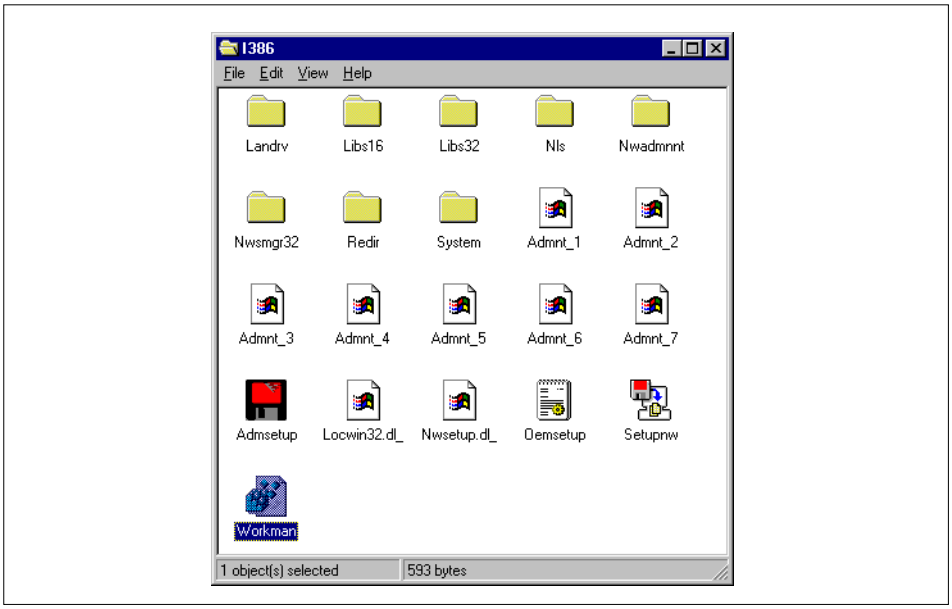


Figure 101. I386 Folder's Contents

10. Click on the **Admsetup** icon and the following message appears:

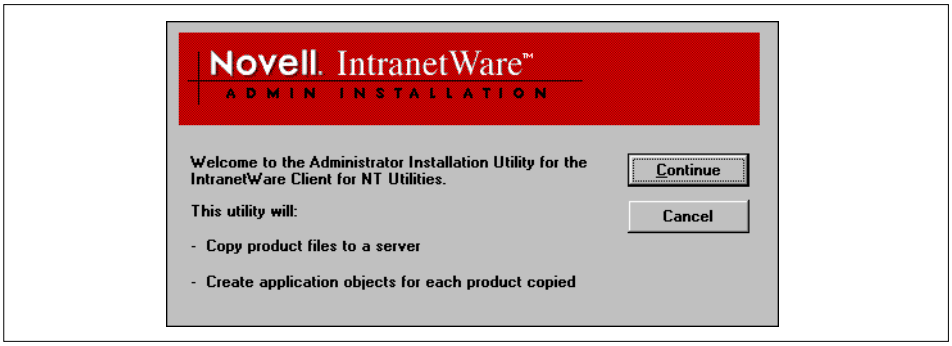


Figure 102. Novell IntraNetWare Administrator Installation Window

11. This utility will copy product files to the server we choose and will create application objects for each product copied. Figure 103 shows the Setup Selections window.

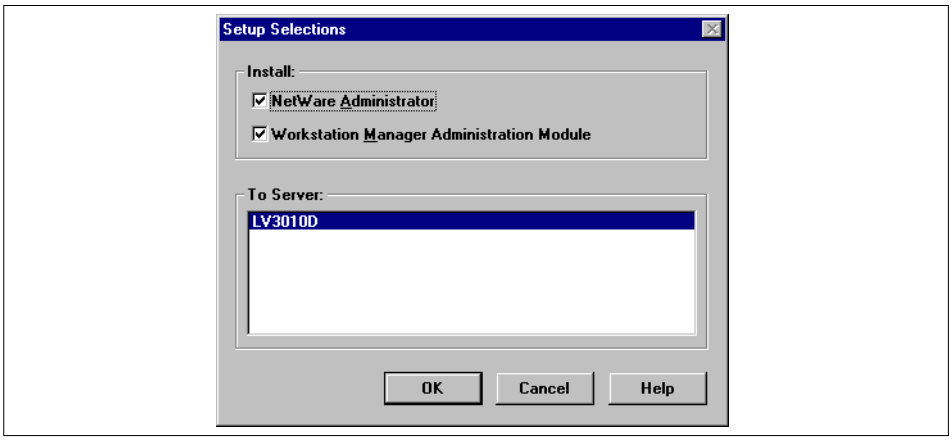


Figure 103. Setup Selections Windows

12. We select our server (lv3010d in our example) and continue with the installation. Setup requires a minimum of 47 MB of free space on the volume /ncps/sys belonging to the NNS server. At the end of the installation, the following window appears:

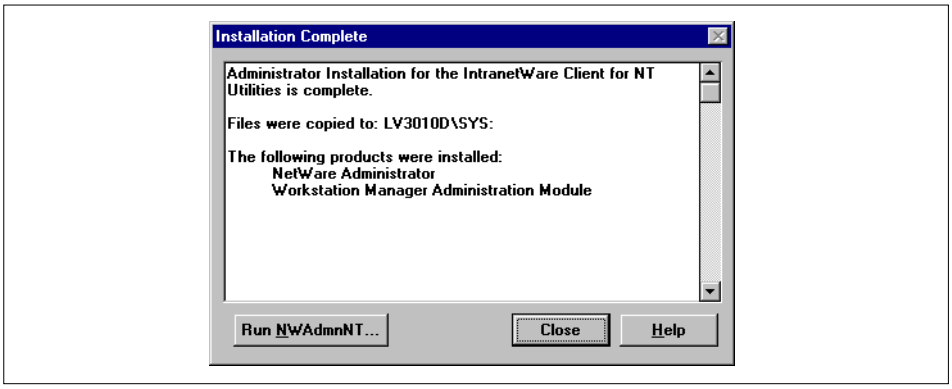


Figure 104. Installation Complete Window

5.9 Configuring Printer Support

The printing capabilities of NNS allow us to share print resources among NetWare clients. Referring to Figure 105, when a user sends a print job from a NetWare client workstation, the print job travels across the network and arrives at the NNS server, where it is stored in as a file in a designated NetWare directory (/ncps/sys/queues/xyxyxyxy.qdr). This directory is called a print queue. Print queues are assigned to network printers. The print job resides as a file in the print queue until the network printer is ready. The print server monitors the print queues and transfers pending print jobs from the queues to the printers. There are two different types of network printers:

- A local printer is attached to the AIX machine or AIX print queue.
- A remote printer is attached to a PC client or a UNIX client.

Network printers require a port driver to print network print jobs. NNS provides two types of port drivers: NPRINTER.EXE and the NPRINTER daemon. Network printers attached to Windows NT workstations require NPRINTER.EXE to be running on the workstation. Network printers attached to NNS servers require the NPRINTER daemon to be running on the server. The NPRINTER daemon is an AIX process that allows printers defined through the AIX print system to service the print server.

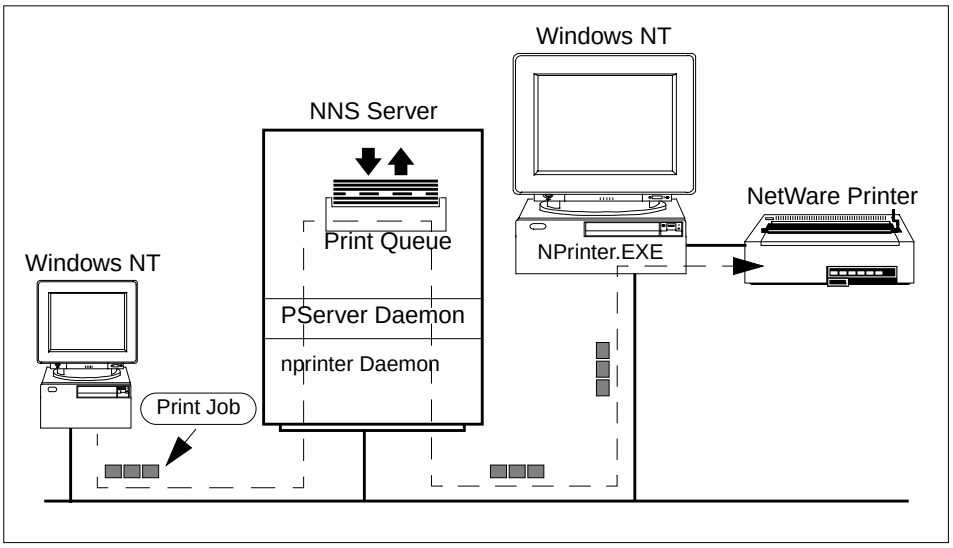


Figure 105. Printers Scenario

In this section we discuss what we must do on the NNS server (RS/6000) and on the client (Windows NT) to configure these two types of printers. To do so, we have already installed at least one PC client (see Section 5.8)

5.9.1 Local Printer Configuration

If we are configuring a printer attached to the RS/6000 machine running NNS, the print server, print queues and printers should be already configured in AIX. We can use SMIT panels to configure local and remote AIX printers and print queues. In the following example the local AIX queue name is ps1.

5.9.1.1 Client Configuration

To configure a printer attached to the AIX machine, on a PC running Windows NT, we use the PC client tool **pconsole**. This tool is an executable provided with NNS in the SYS volume, public folder. The following is the procedure to configure a printer using pconsole:

1. In a PC window, run the `pconsole` command and the following panel appears:

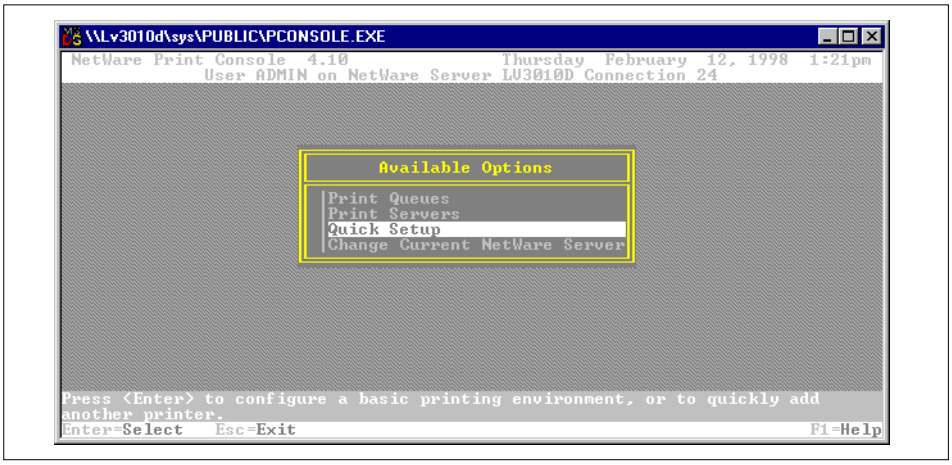


Figure 106. pconsole Panel

2. Select **Quick Setup** and the following panel appears:

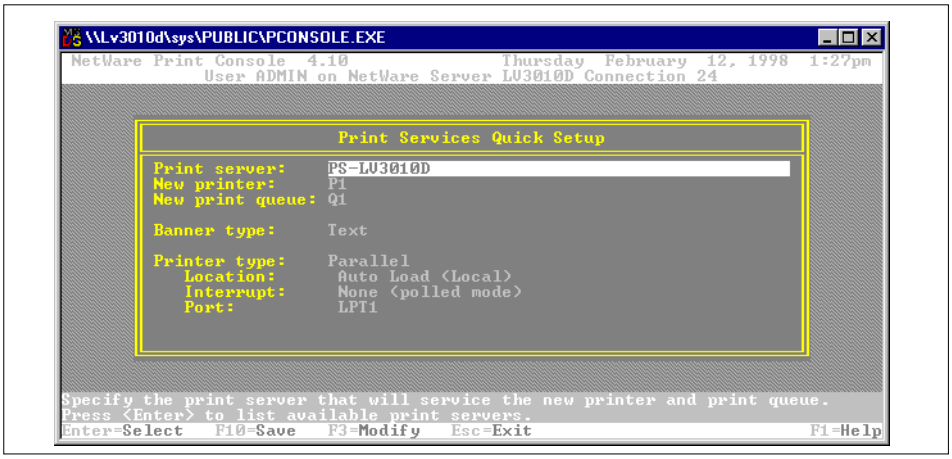


Figure 107. Print Services Quick Setup Panel

3. In our example we are adding a print server named `PS-lv3010d`. We choose the default values for all the fields except for the Location field that we changed to auto-load. It specifies how the printer driver will load. Only printers cabled to the print server can auto load. We have to press the **F10** key to save our object.
4. On the pconsole main menu, select **Print Servers**, as shown in Figure 108.

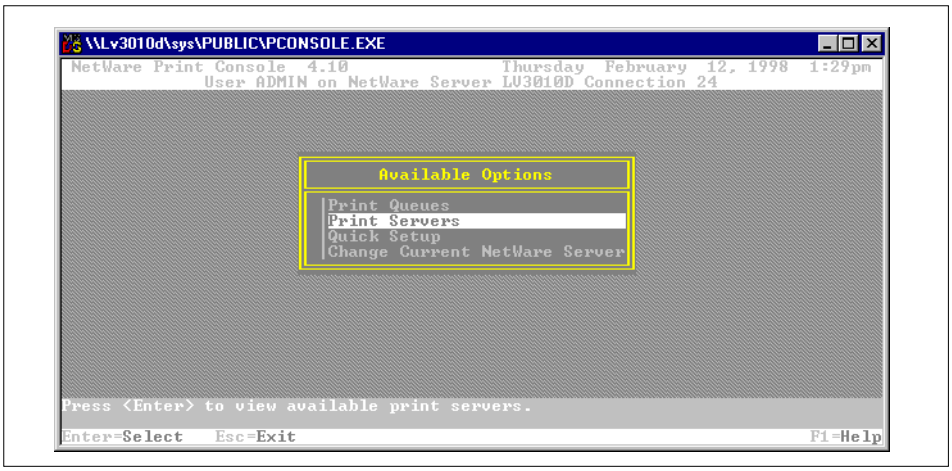


Figure 108. Print Servers Panel

5. Press the **Enter** key on the Print Servers list and then select **Password**, as shown in Figure 109.

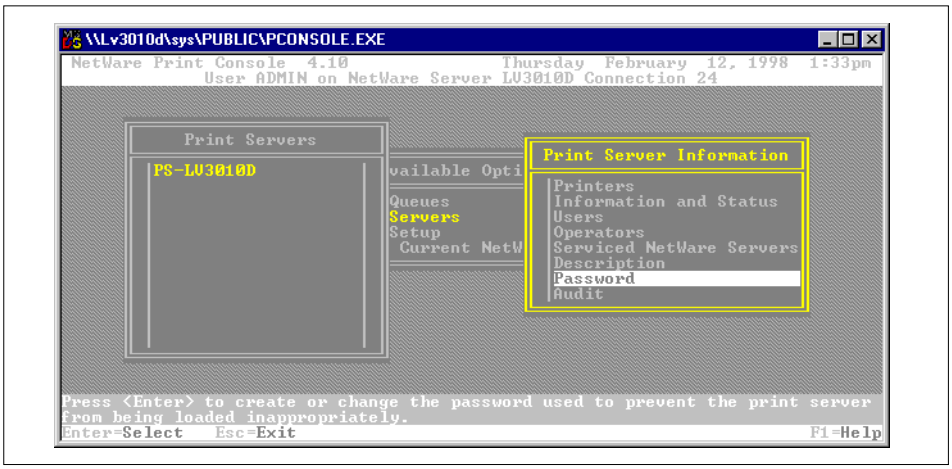


Figure 109. Print Server Password

6. If a password is assigned to a print server, that password must be entered every time the print server is loaded. A password prevents unauthorized attempts to attach as a print server to gain the security equivalence of a print server.
7. Make a note of the information you supply for the print server name, printer name, queue name and password. You need this information for the configuration on the NNS server.

8. Click on the server folder to see the resources available for the PC, including the queue Q1 we just configured (Figure 110).

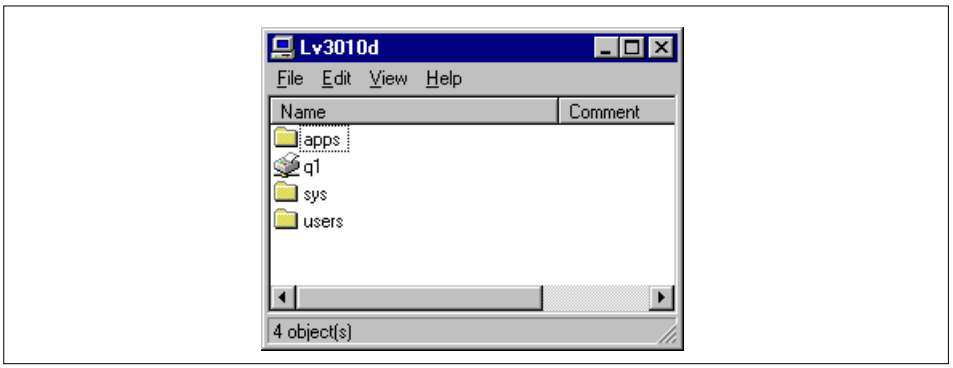


Figure 110. NNS Resources Window

9. Click on the **Q1** icon to add this queue to the PC client. The following message will appear:

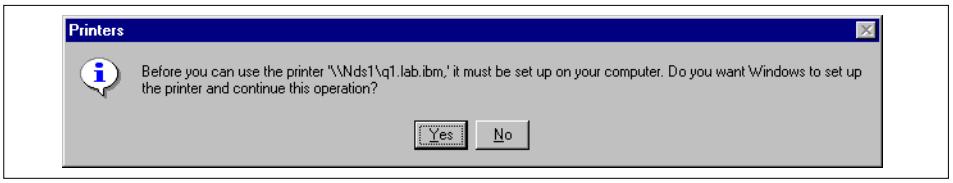


Figure 111. Printer Message

10. If we look in the Printer folder of our PC client at the end of the installation, we will see the print queue, Q1, available. To use it, we have to configure the NNS server running on the RS/6000 system, as described in the following section.

5.9.1.2 NNS Server Configuration

The following is the procedure to configure the print server on the NNS server running on the RS/6000 system.

1. Type `smit ncps` and select **Further Configuration**-> **Print Server** to get the following panel:

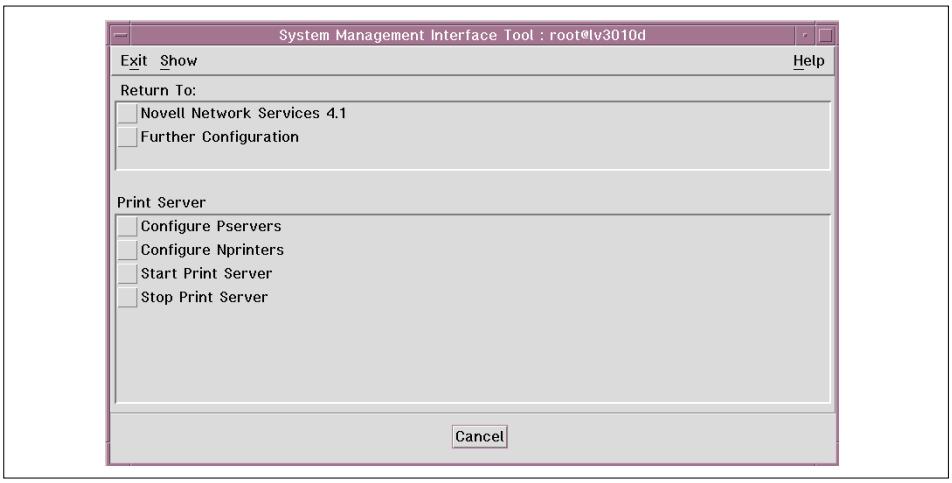


Figure 112. Print Server Panel

2. Select **Configure Pservers** and the following panel appears:

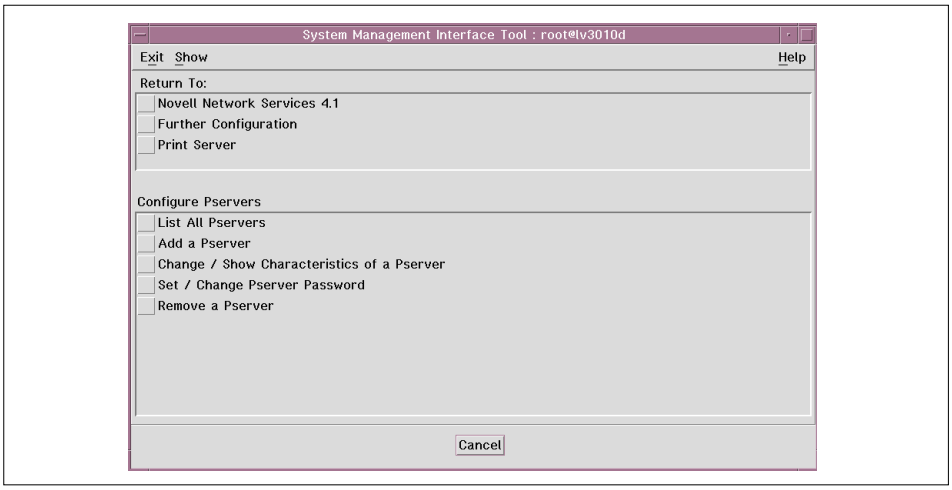


Figure 113. Configure Pservers Panel

3. Select **Add Pserver** and complete the field as shown in Figure 114. All the values are related to the configuration on the client using pconsole. The Printer Number field is related to a number that pconsole associates with

the printer (usually 0 is associated with the pair P1 and Q1, 1 is associated with the pair P2 and Q2, and so on). Click on **OK** to save the Print Server configuration.

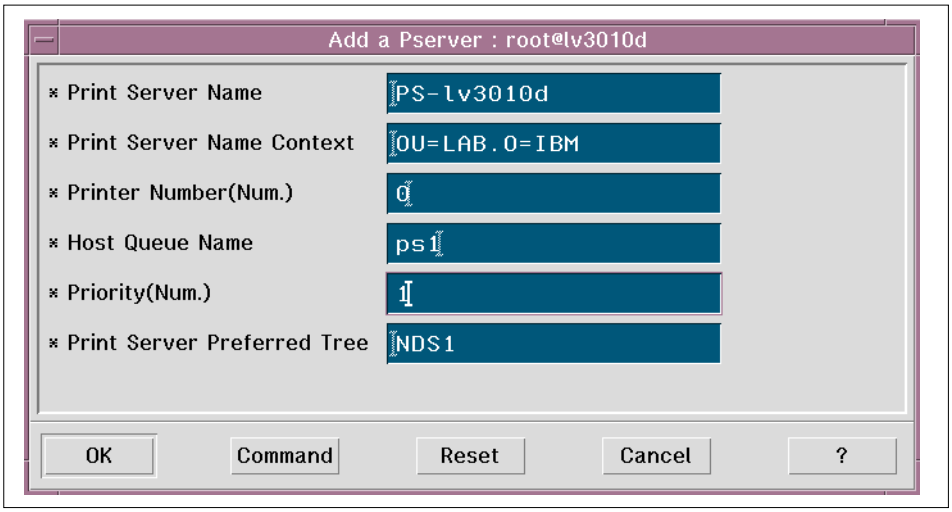


Figure 114. Add Pserver Panel

4. Now we must configure a printer server password (the same password entered on pconsole panel). Select **Print Server** -> **Configure Pservers** and choose the print server from the list (Figure 115).

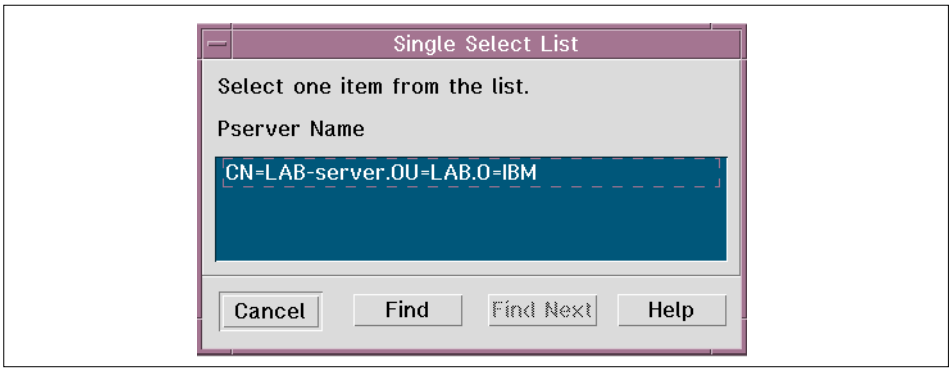


Figure 115. Lists of Print Servers

5. Select from the list and the following panel is displayed:

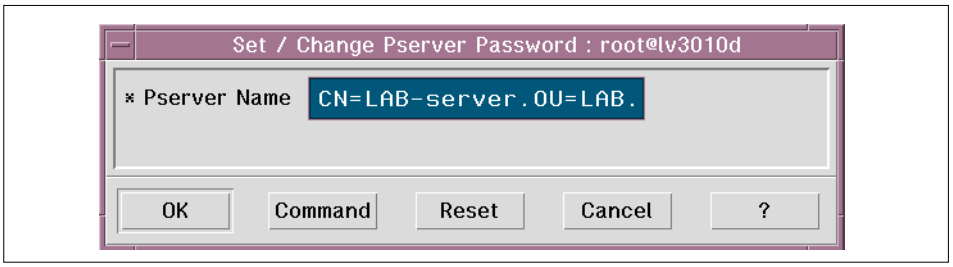


Figure 116. Print Server Password

6. Now we are ready to start the Print Server daemon on our NNS server. The name of the Print Server daemon is PServer. To start the PServer daemon from SMIT, select **Further Configuration** -> **Print server** -> **Start Print Server**. From the smit panel it is also possible to stop the PServer daemon. To do this, select **Further Configuration** -> **Print Server** -> **Stop Print server**. To start, restart and stop the PServer daemon from the command line use the following commands:

- `nw start printer`
- `nw restart printer`
- `nw stop printer`

Note

Print logging is saved in the file /var/ncps/pserver/pserver.log.

5.9.2 Remote Printer Configuration

A remote printer is a printer attached to a NetWare client workstation on the network, or directly to the network itself. We must configure the printer to the Windows NT PC that will be our print server before adding remote printer entries.

5.9.2.1 Client Configuration

We must define a NetWare printer and queue for a remote printer using the pconsole tool. This tool is an executable provided with NNS in the SYS volume, public folder. The following is the procedure to configure a printer using pconsole:

1. In a PC window, run the pconsole command and the following panel appears:

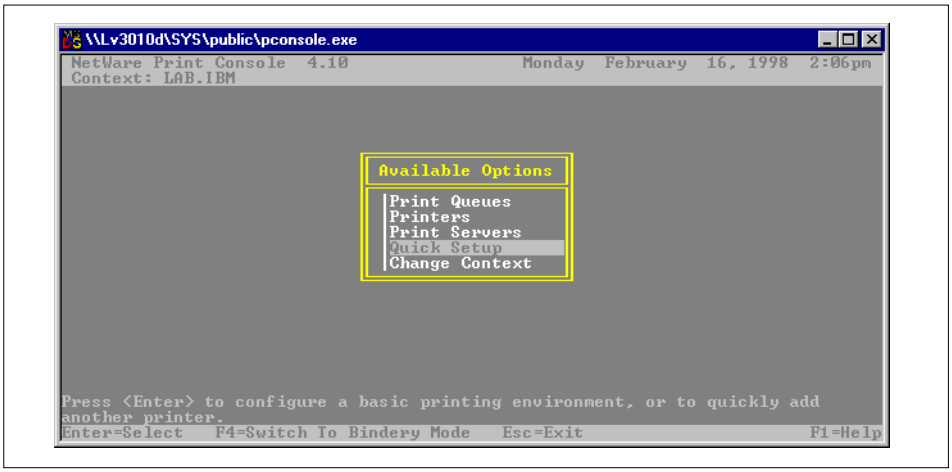


Figure 117. pconsole Panel

2. Select **Quick Setup** and the following panel appears:

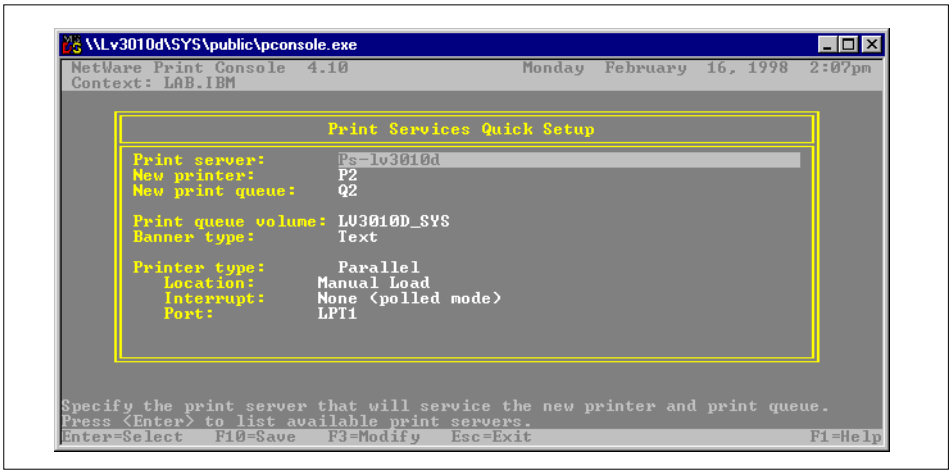


Figure 118. Print Services Quick Setup Panel

3. Define a new printer and print queue. The pconsole increments the default numbers for the printer and print queue on the screen. Leave the location field as Manual Load. We have to press the **F10** key to save our object.

4. Click on the server folder to see the resources available for our PC, including the queue Q2 we just configured (Figure 119).

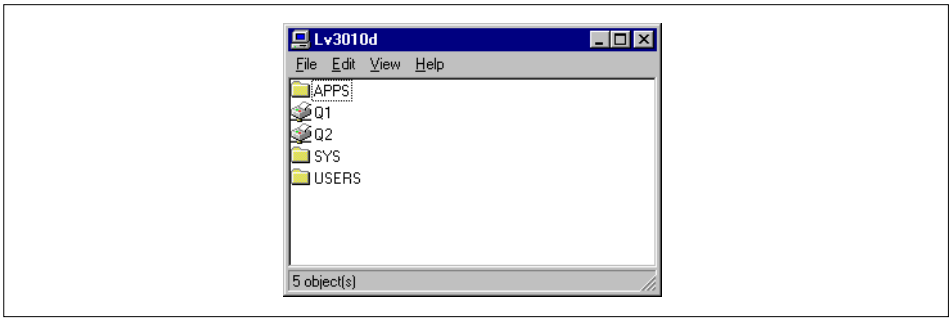


Figure 119. NNS Resources Window

5. Click on the **Q2** icon to add this queue to the PC client. The following message will appear:

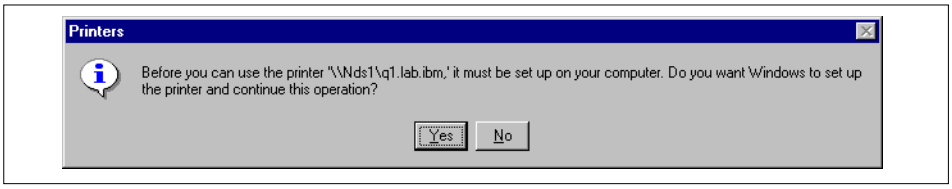


Figure 120. Printer Message

6. At the end of the installation in the Printer folder of our PC client we will see the print queue Q2 available. To use it we have to configure the NNS Server running on the RS/6000 system as described in the following section.

5.9.2.2 NNS Server Configuration

The following is the procedure to configure a remote printer to the NNS server running on the AIX machine:

1. Type `smit ncps` and select **Further Configuration**-> **Print Server**-> **Configure Nprinters** to get the following window:

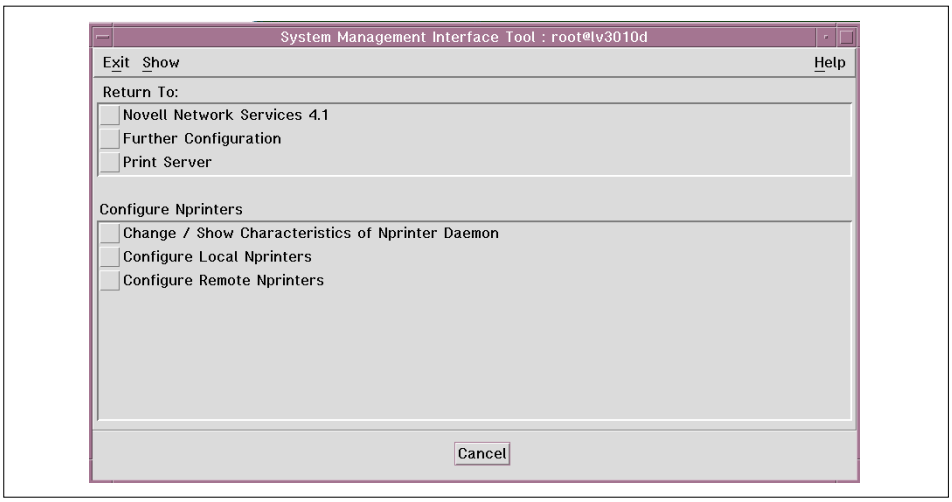


Figure 121. Configure Nprinters Window

2. Select **Configure Nprinters** -> **Add a Remote Nprinter** and the following window appears:

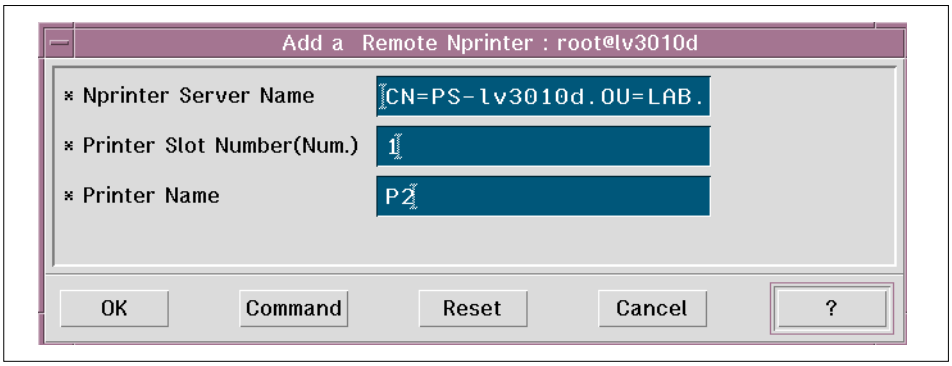


Figure 122. Add a Remote Nprinter Window

3. The Printer Slot Number and Printer Name fields must be the same values, as configured by pconsole. Click on **OK** to save the configuration.
4. Now we are ready to start the Print Server daemon on our NNS server running on the RS/6000 machine. If the Pserver daemon has already been started, we must restart it. The name of the Print Server daemon is

PServer. To start the PServer daemon from SMIT, select **Further Configuration** -> **Print server** -> **Start Print Server**. From the SMIT panel it is also possible to stop the PServer daemon. To do this, select **Further Configuration** -> **Print Server** -> **Stop Print server**. To start, restart and stop the PServer daemon from the command line, we can use the following commands:

- `nw start printer`
- `nw restart printer`
- `nw stop printer`

Note

Print logging is saved in the file /var/ncps/pserver/pserver.log.

5. On the PC that will be our print server, we have to run the `nprinter` command to configure the queue. This tool is an executable provided with NNS in the SYS volume, public folder. In a PC window, run the `nprinter` command and the following window appears:

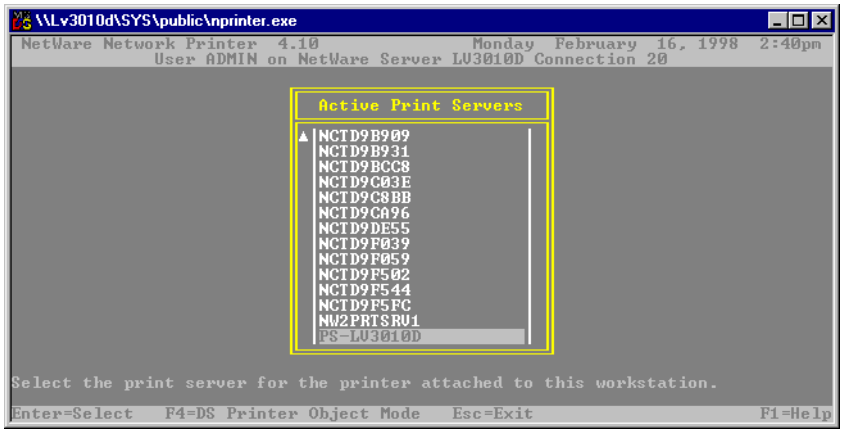


Figure 123. nprinter Windows

6. Select the server and the following window with the available printers appears:

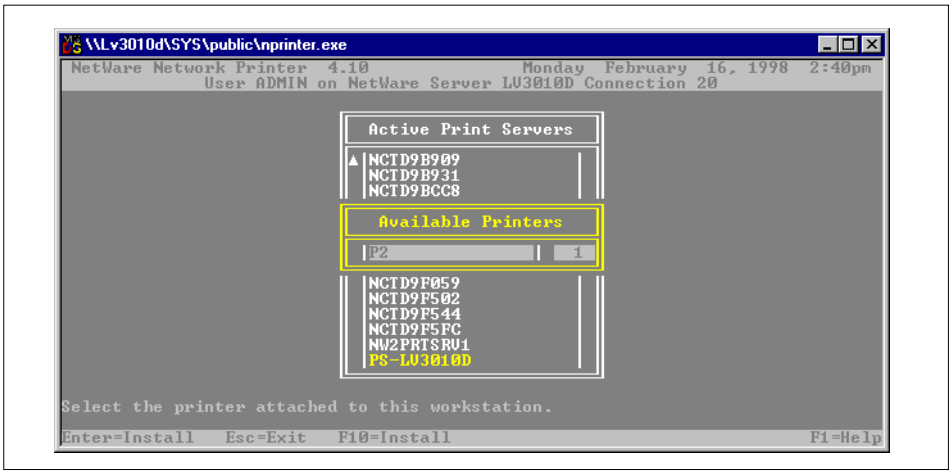


Figure 124. Available Printer Window

7. Select the printer attached to your PC and then press **Enter**. The following panel appears:

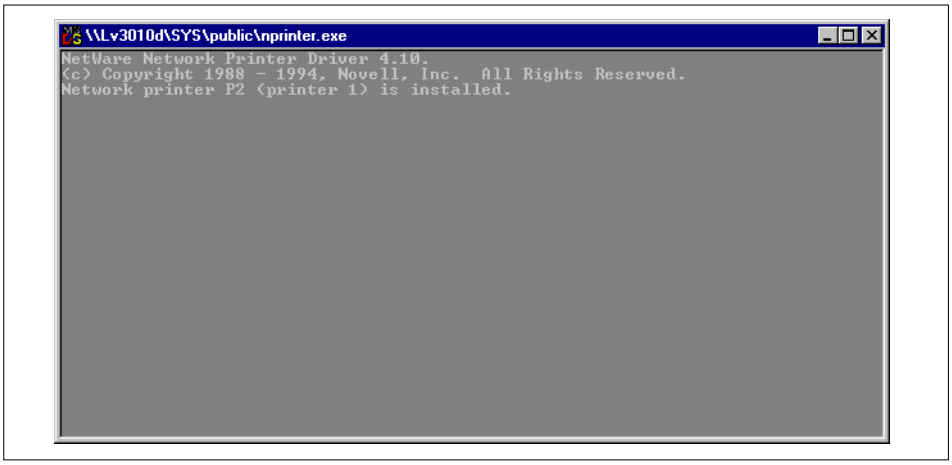


Figure 125. Starting nprinter

Note

The queued print jobs will be located in the /ncps/sys/queues/xyxyxyxy.qdr file.

5.10 Client Operations

In this section we discuss how to operate with the Novell intraNetWare Client 4.11a for Windows NT 4.0. The same procedure can be followed for the Window NT 4.0 NetWare Client and Gateway, although at the moment this software has some problems that need to be fixed (see Section 5.13 on page 181).

5.10.1 How to Map a Drive

We created volumes on the NNS server and we want to map one volume as a drive for our Windows NT workstation. To do this, follow these steps:

1. From the Windows NT desktop, click on the **Network Neighborhood**. The following window appears:

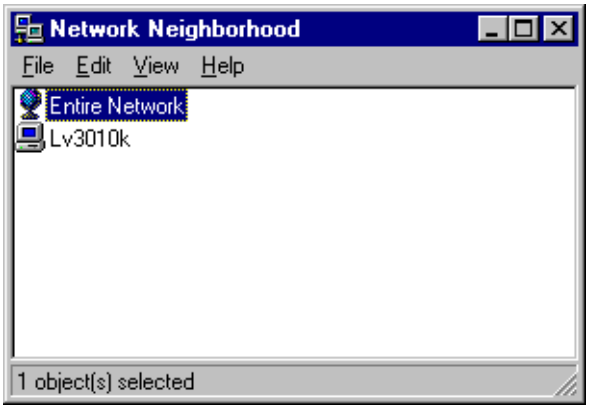


Figure 126. Network Neighborhood Window

2. Click on **Entire Network** and then from **NetWare or Compatible Network**, open your NNS server as shown in Figure 126.

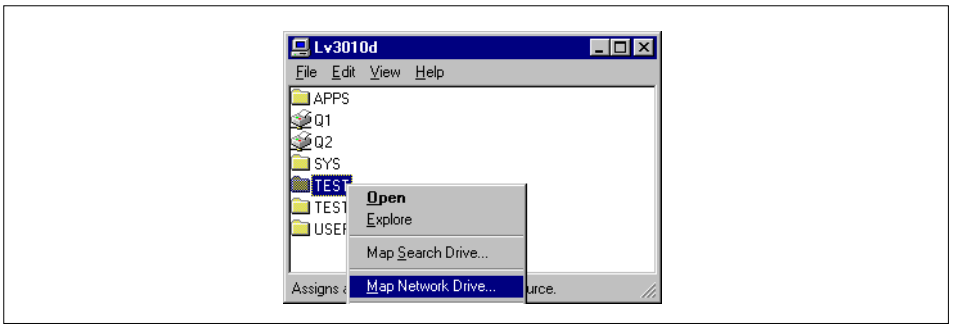


Figure 127. Available Resources Window

3. Select the volume you want to map and using the right mouse button, select **Map Network Drive**.The following window appears:

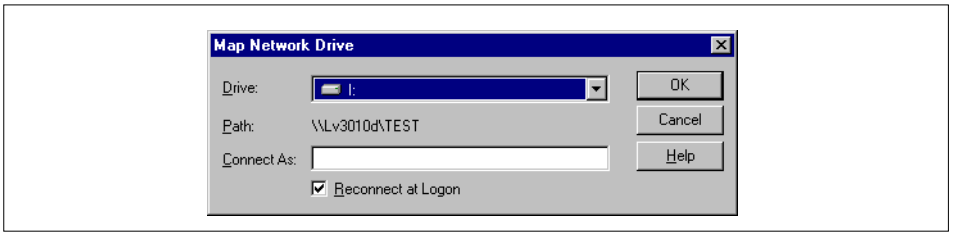


Figure 128. Map Network Drive Window

4. Choose the drive letter to associate with the volume and then click on **OK**. To check that the configuration was successful, from the Windows NT desktop click on the **My Computer** icon. The following panel appears:

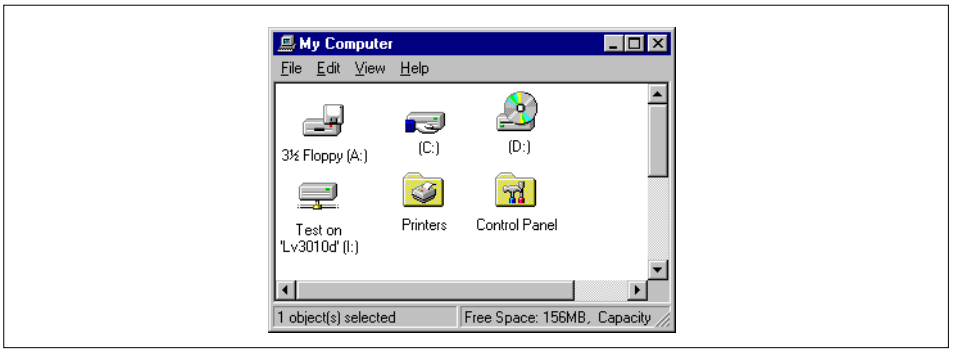


Figure 129. My Computer Windows

5.10.2 How to Create a User

To create a new Novell's user, follow these steps:

1. From the Public folder in the SYS volume, select the **winnt** folder and the following window appears:

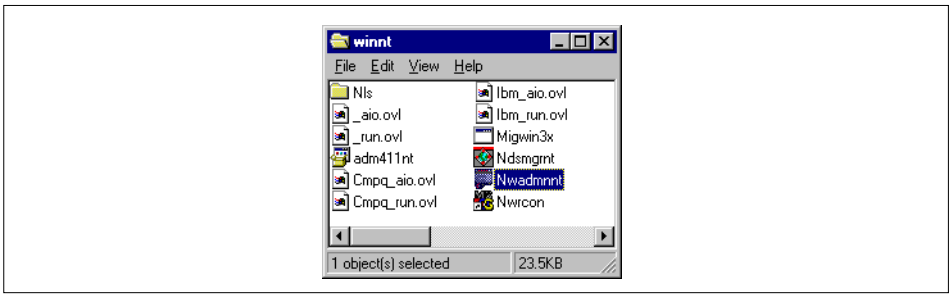


Figure 130. winnt Folder

2. Click on the **Nwadmnnt** icon and the NetWare Administrator program shows the following window:

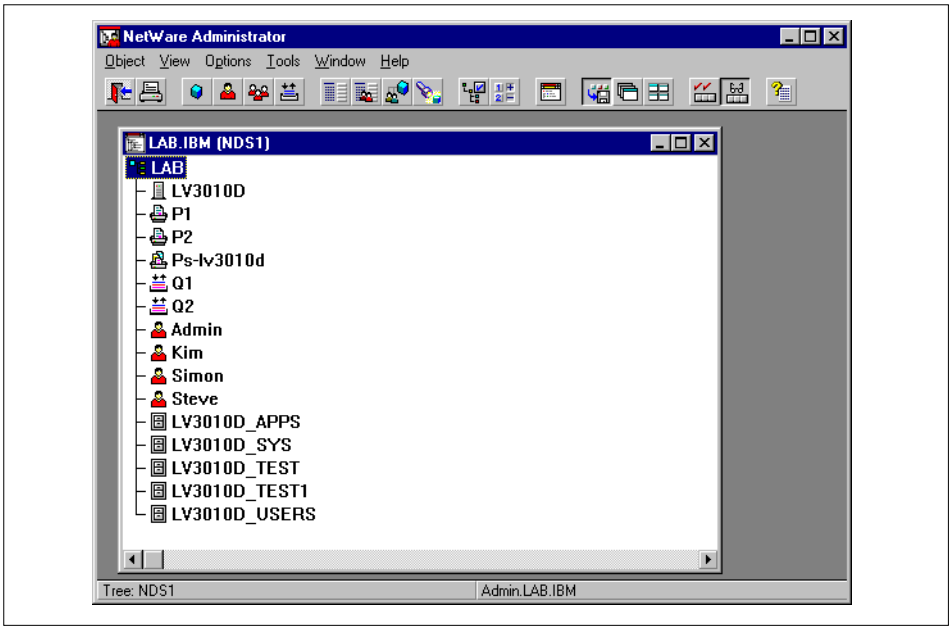


Figure 131. NetWare Administrator Window

3. Figure 131 shows the content of our context. Select **Create** from the **Object** menu and the following window is displayed:

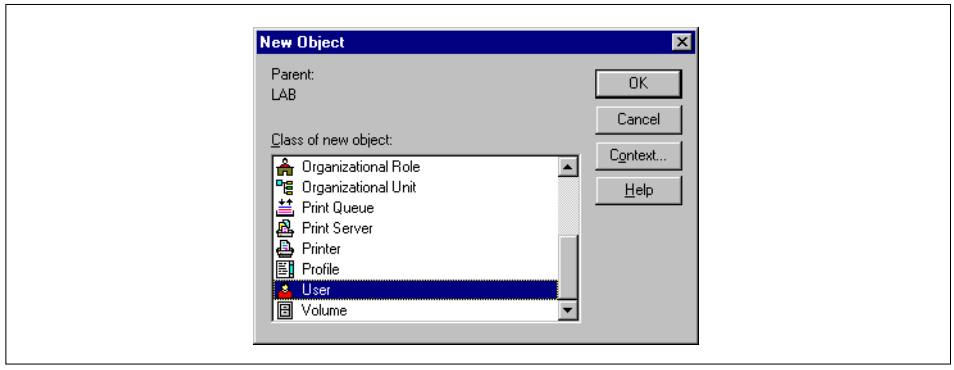


Figure 132. New Object List

4. From the New Object window select **User** and the following panel appears:

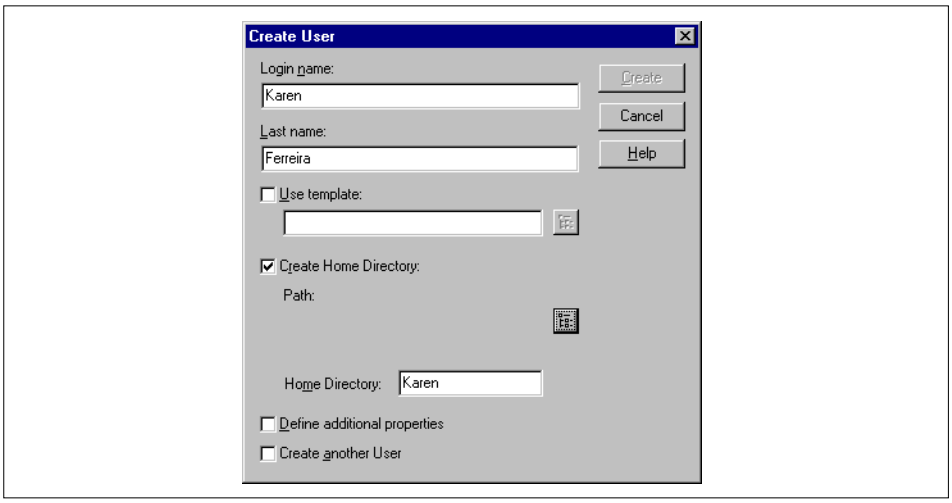


Figure 133. Object User Panel

5. Choose the Login name and the Last name and, if you want, Create Home Directory. If we select **Create Home Directory** the following panel appears:

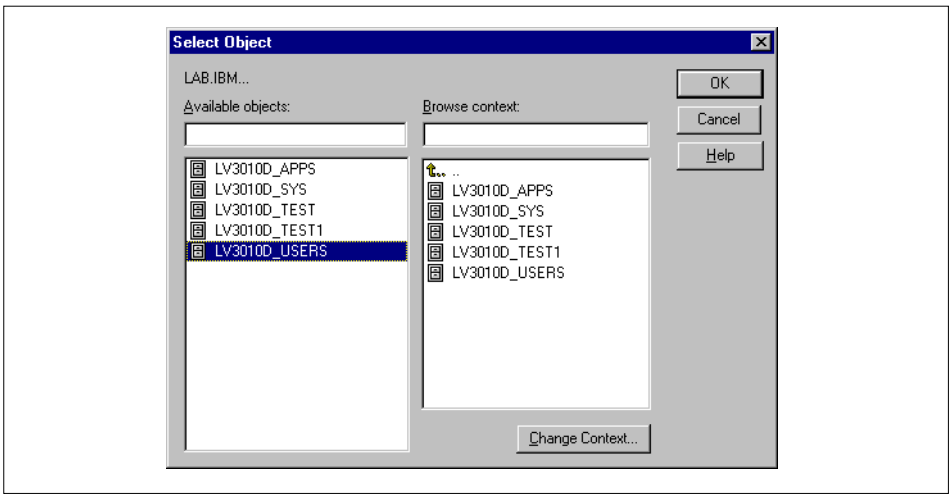


Figure 134. Volume Object

6. Choose the volume in which you want the home directory to reside. Click on **OK** to confirm your choice. The NetWare Administrator window now shows the new user, as shown in Figure 135.

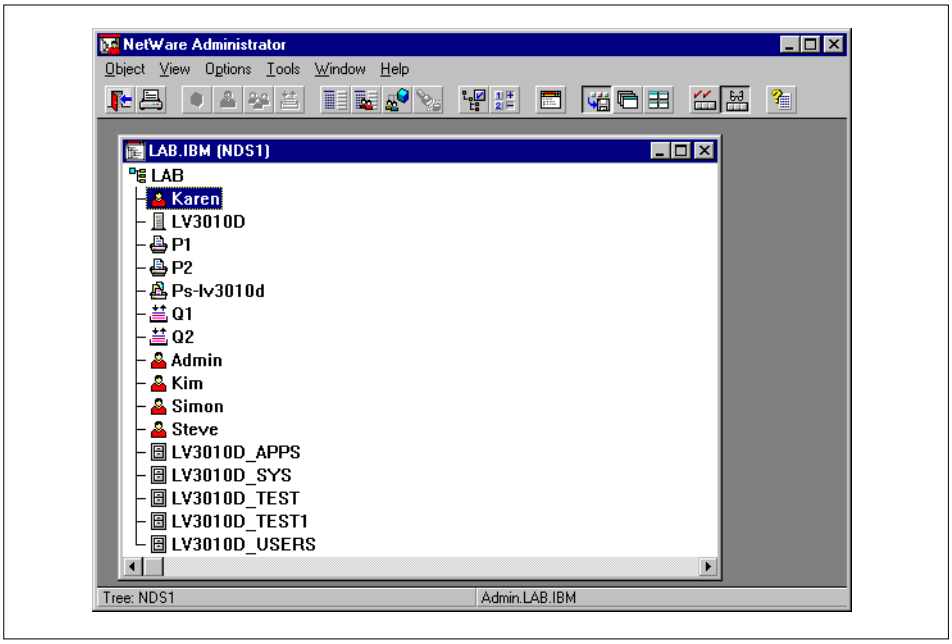


Figure 135. NetWare Administrator Window

5.10.3 How to Set a User's Properties

From the NetWare Administrator window, double-click on the desired user's icon and the following panel appears:

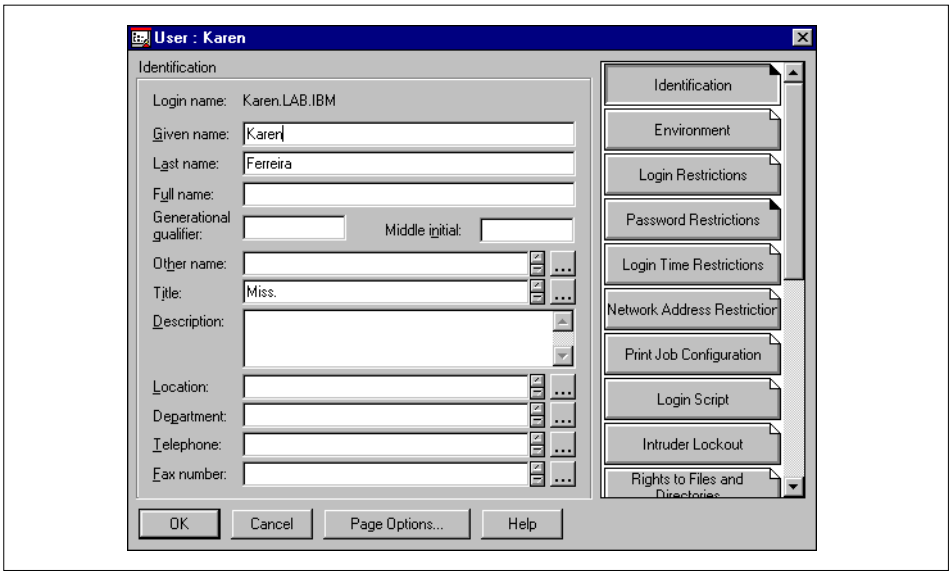


Figure 136. User Panel

From this panel it is possible to set several properties. We are going to set Password Restrictions for the user, as shown in Figure 137.

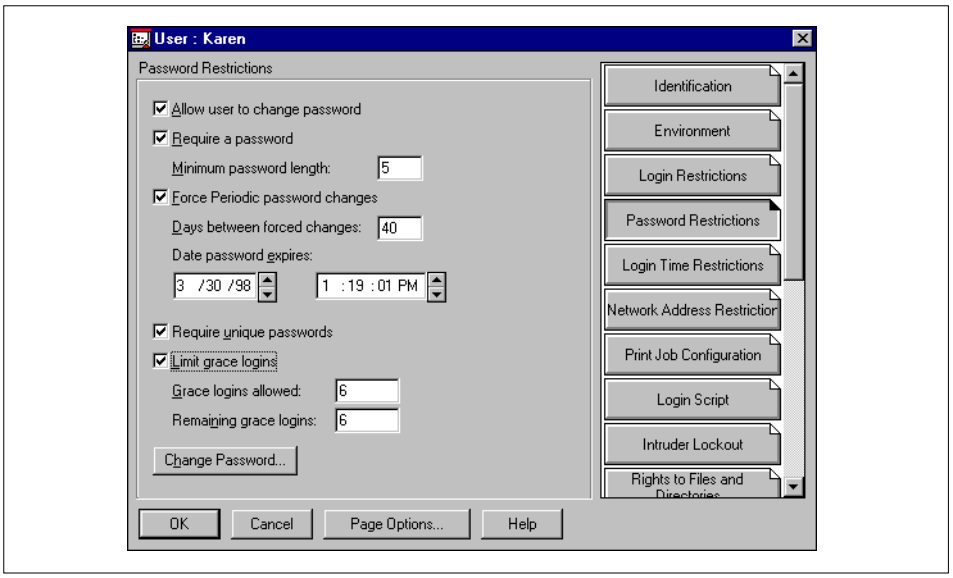


Figure 137. Setting User's Password Panel

We can also set the Security for the user to be equal to Admin. Click on the **Security Equal To** button and then choose the level of security to grant to our user (Figure 138).

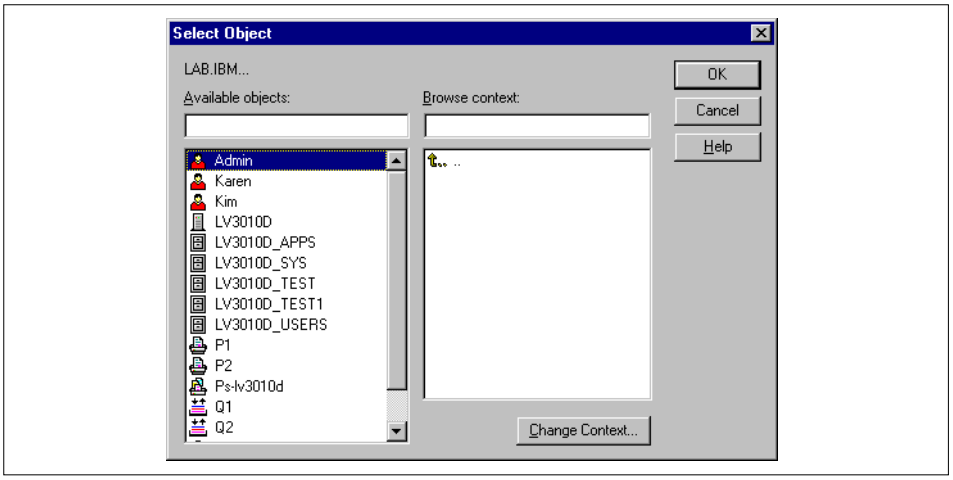


Figure 138. Security Equal to Window

In our example for user Karen we chose the Admin Security level, as shown in Figure 139.

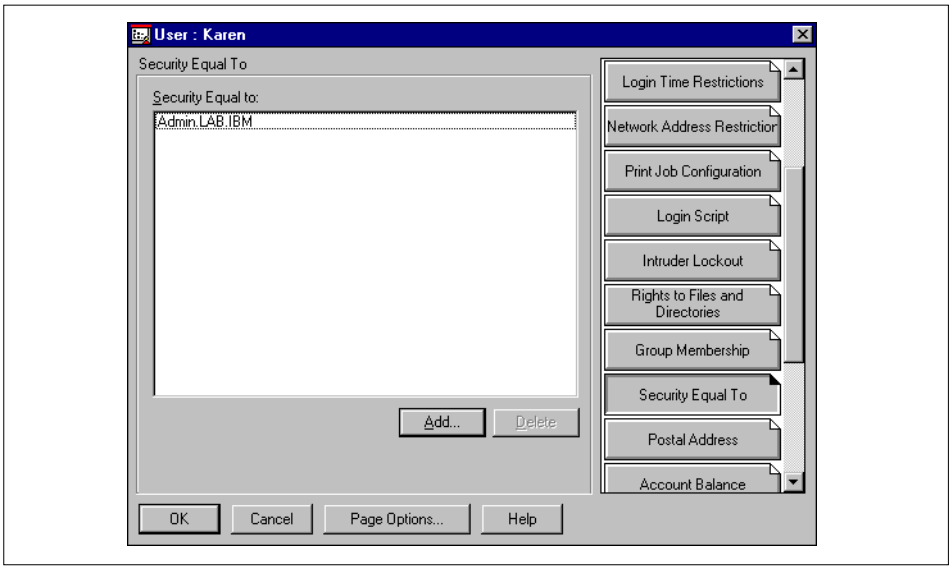


Figure 139. User Windows

5.10.4 How to Create a Group

It is possible to create a group of users. To do so, follow these steps:

1. Click on the **Nwadmnnt** icon and the NetWare Administrator program shows the following window:

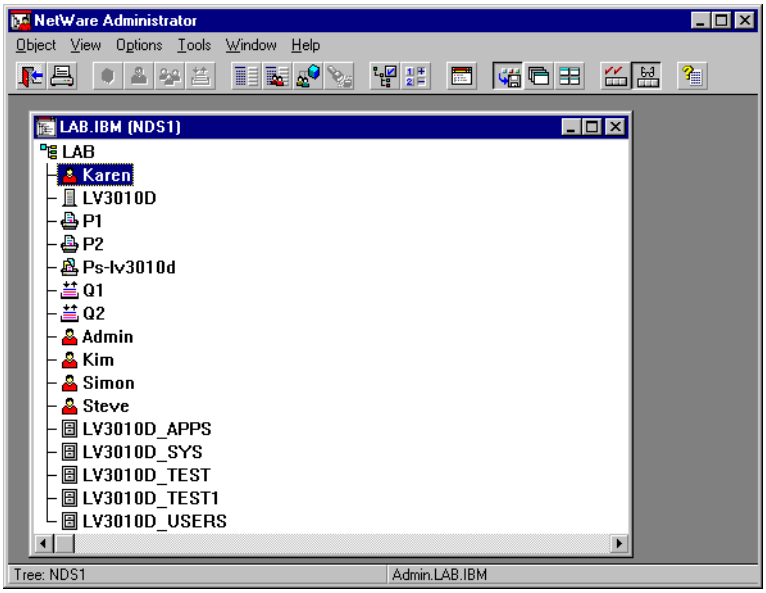


Figure 140. NetWare Administrator Window

2. Select **Create** from the **Object** menu and the following window appears:

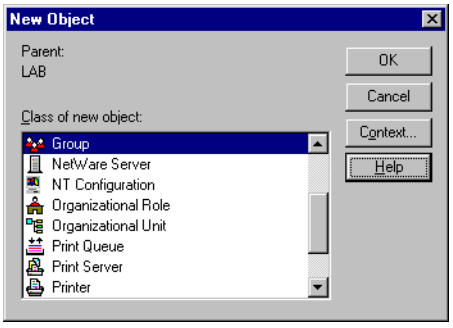


Figure 141. New Object Window

3. Choose an appropriate name for the group and then select **Create** (Figure 142).

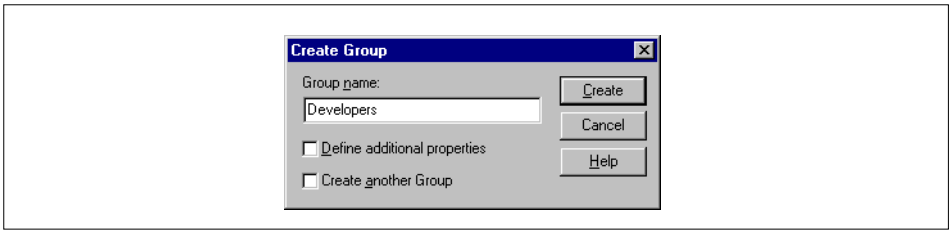


Figure 142. Create Group Window

4. The NetWare Administrator window shows the new group, as shown in Figure 143.

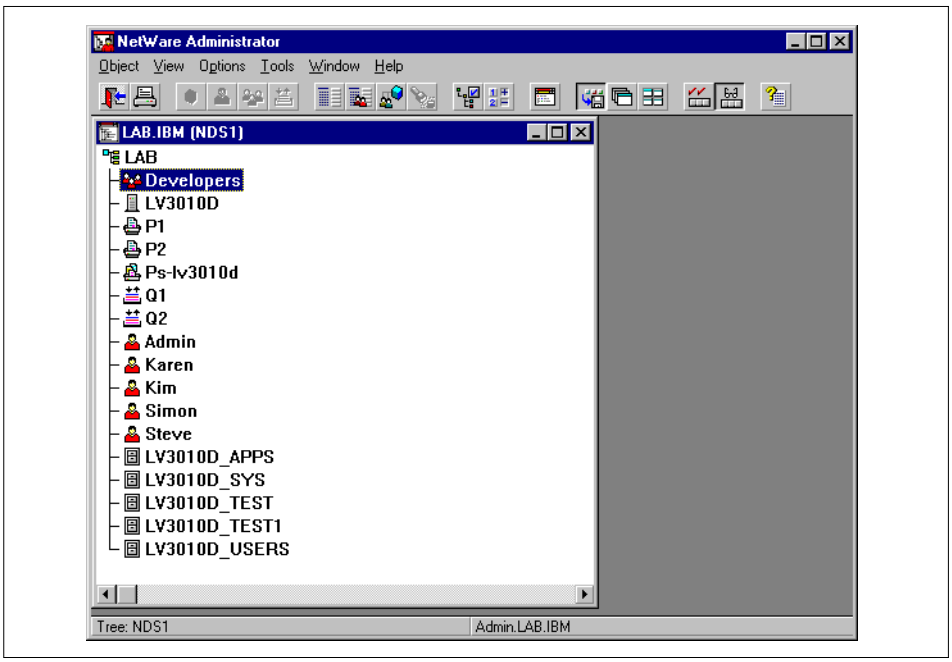


Figure 143. NetWare Administrator Window

5. From the NetWare Administrator window, double-click on the group's icon, Developers in our example, to set properties. The following window appears:

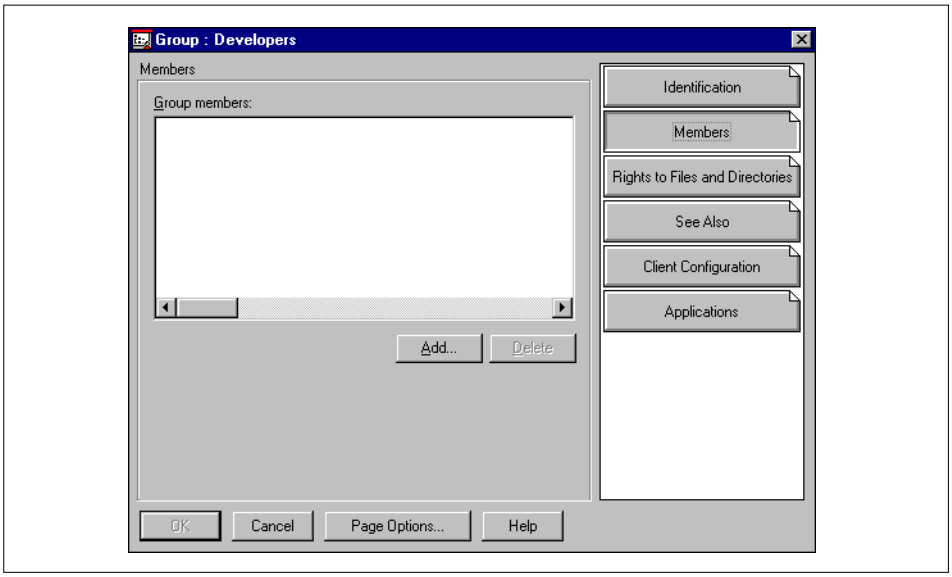


Figure 144. Group Window

6. From this window, it is possible to set several properties. We are going to set members for the group. As shown in Figure 145, we can choose the users that will belong to the group.

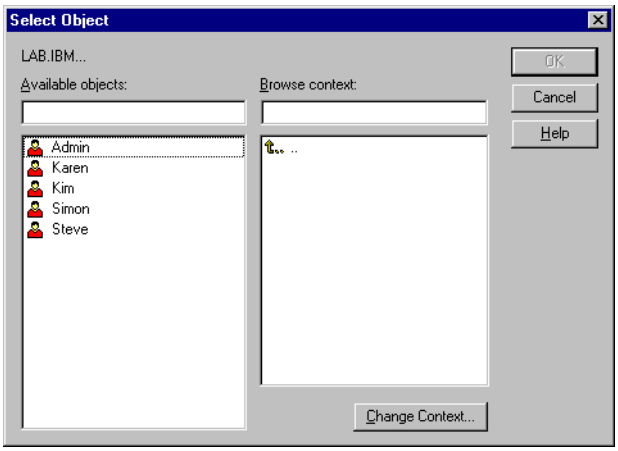


Figure 145. Available Users Window

7. In our example the users Karen, Simon and Steve have been added to the Developers group (Figure 146).

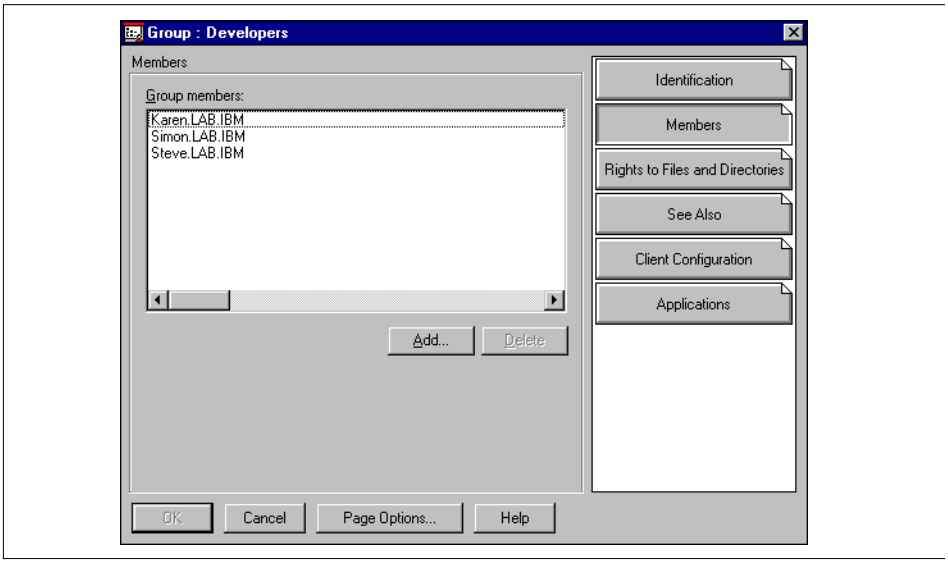


Figure 146. Group Window

8. We can set the rights to files and directories for the members of the group we created. Click on the **Right to Files and Directories** button. Click on the **Find** button to see the available volumes. Select one volume and click on the **Add** button. As shown in Figure 147, we can set the rights for the chosen volume.

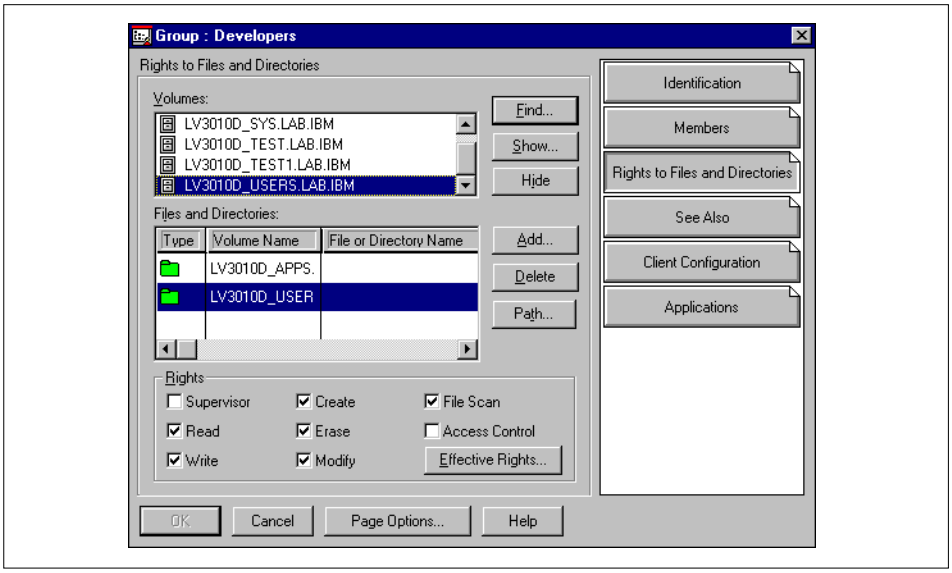


Figure 147. Rights to Files and Directories Window

5.11 NNS processes

The following is a list of the processing involved in an NNS server:

`root timerd` (NWS Timer Daemon)

`root sapd` (IPX Sap Daemon)

`root NWU NVT Server`

`root npsd` (IPX Protocol Stack Daemon)

`root ncp_engine` (NWS NCP Engine)

`root sap` (NWS Server Advertiser)

`root log_lockd` (NWS Logical Lock Daemon)

`root /usr/bin/nprinter`

nwprint NWU PServer

root nucd

root nwserver (NWS Daemon)

root ntsd (NWS Time Synchronization Daemon)

root file_lockd (NWS File Lock Daemon)

root phys_lockd (NWS Physical Lock Daemon)

root sema_lockd (NWS Semaphore Daemon)

root dsbackd (NWS DS Background Daemon)

root dsbackd (NWS DS Background Daemon)

root ssjanitor (NWS DS Janitor Daemon)

root dsskulker (NWS DS Skulker Daemon)

root ncp_engine (NWS NCP Engine)

nwprinter NWU PServer

root nwserver (NWS Daemon)

5.12 Limitations

The following list describes several NNS limitations.

- NNS (5765-C95) is mutually exclusive with AIX Connections (5765-C34 or 5765-655).
- NNS is mutually exclusive with the ipx.rte software package. This LPP is shipped with the AIX Version 4 or later. It provides basic IPX/SPX protocol stacks to use with several applications. You must uninstall ipx.rte before you install NNS and the ipx.base software.
- NNS is mutually exclusive with the 7318 Terminal Server. Compatibility issues with IPX/SPX prohibits the use of the 7318 product.

5.13 Troubleshooting

We experienced some problems using the Microsoft clients (we recommend using Novell clients). The following is a list of two common errors:

- Microsoft client --> The admin setup does not start. Some dll files are missing. Figure 148 shows the error message. To fix this problems, you have to download the dll from the Novell client software.

Figure 148. Setup Admin Error Message

- Microsoft client --> Printer error. When we try to print on a queue belonging to the server, we received the error message shown in Figure 149. This error does not occur with the Novell client.

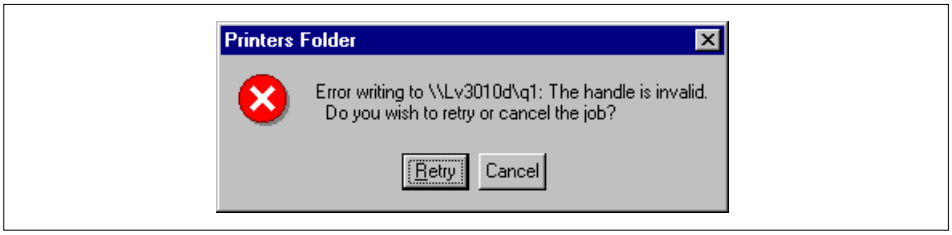


Figure 149. Printer Error Message

5.14 Year 2000

NNS is Year 2000-ready. When used in accordance with its documentation, it is capable of correctly processing, providing, and/or receiving date data within and between the twentieth and twenty-first centuries, provided all other products used with the product properly exchange date data.

Chapter 6. Advanced Server for UNIX

Advanced Server for UNIX (AS/U) on AIX is an implementation, by Group Bull, of AT&T's networking operating system. AS/U provides AIX with networking features equivalent to Windows NT Server.

6.1 Advanced Server for UNIX Overview

AS/U enables UNIX systems to act as a server for PC Client systems (MS-DOS, OS/2, Windows, Windows for Workgroups, Windows 95 and Windows NT Workstation). Through an exclusive joint development agreement with Microsoft, which includes delivery of Windows NT source code, AT&T has been able to produce a product that gives functionally equivalent networking features to Windows NT Server. The AIX version of AS/U has been produced by Group Bull.

Central to AS/U is the Server Message Block (SMB) protocol that enables clients and servers to exchange messages and data. AS/U does not require code to be installed on client systems. As far as the clients are concerned, they do not know whether they are using an NT or AS/U server.

AT&T began it's relationship with Microsoft in 1991 when it delivered a product providing LAN Manager networking on UNIX. This product has now evolved into AS/U (the first release was provided to OEMs in December 1994). The exclusive agreement with Microsoft will allow AT&T to implement future changes of Windows NT networking into AS/U. Provided that the relationship continues, this will allow the major versions of UNIX to interoperate with current and future versions of Microsoft operating systems in a highly-integrated way.

6.1.1 AS/U Features

The key Windows NT interoperability features that AS/U offers are:

- SMB-based client support
- Logon validation
- File system access control
- Print serving (local and remote)
- Remote administration
- Primary or backup domain controller
- WINS Server

- Inter-domain trust relationships
- Account and file replication

6.1.1.1 SMB-Based Client Support

AS/U supports Windows NT clients using the Server Message Block protocol. Windows NT systems communicate with AS/U using NetBIOS over TCP/IP. This is the default network protocol for Windows NT systems and therefore no extra code is required on the client or participating systems to be able to use and communicate with the AS/U server.

6.1.1.2 Logon Validation

AS/U supports Windows NT logon validation. Acting as a primary domain controller, AS/U can be configured with user accounts that are used by Windows NT systems in the domain to log on users. User and password authentication is provided by the AS/U server. Acting as a backup domain controller, AS/U can provide logon validation for user accounts that have been replicated from primary domain controllers.

6.1.1.3 File System Access Control

AS/U provides Windows NT-style file access control through the use of permissions for groups and users. This means that you can map AS/U users to individual AIX system users and use standard AIX file permissions to give them file access control.

6.1.1.4 Print Serving (Local and Remote)

AS/U allows any AIX print queue to be accessed by Windows NT clients. This enables local or remote printers configured on the AS/U server to be used. If the print queue on the AS/U server is to a remote printer, clients do not have to have permissions on the remote print server to be able to print. AS/U also supports storage of Windows NT printer drivers so that when a client wants to use a printer configured on the AS/U server, they will have the Windows NT drivers downloaded automatically.

6.1.1.5 Remote Administration

AS/U can be administered (with some limitations) directly on the AIX system where it is installed (for instance, when adding and removing users). AS/U also supports the use of the Windows NT server tools which allow the remote administration of the AS/U server, including:

- Account administration
- Trust relationships
- Directory replication

- Printer administration

AS/U also provides a setup of administrative tools (as provided with Windows NT server) that can be installed on a Windows NT system to allow administration of an AS/U server from any Windows NT workstation.

6.1.1.6 Primary or Backup Domain Controller

AS/U can be configured as either a primary or backup domain controller within a Windows NT network. The role of the AS/U server can be changed without reinstalling AS/U.

6.1.1.7 WINS Server

AS/U can be configured as a Windows Internet Naming Service server. This allows AS/U to provide IP addresses for computer names which are requested by client systems. The AS/U WINS server supports replication to and from other WINS servers on the network through the use of push and pull partners.

6.1.1.8 Inter-Domain Trust Relationships

AS/U can participate in Trust relationships with other Windows NT domains.

6.1.1.9 Account and File Replication

AS/U will replicate user account information to backup domain controllers on the network. This reduces the overall load on the primary domain controller. In addition, AS/U provides the directory replication service, which allows files and directories to be replicated from the AS/U server to other AS/U or Windows NT systems in the network.

6.1.2 AS/U Scenarios

As AS/U contains key Windows NT Server networking features, existing UNIX- based customers can provide Windows NT workstations to users without having to change their servers. In addition, existing Windows NT customers who require UNIX servers for increased performance, larger scale systems, clustering, High Availability and so forth, can integrate the new systems using their current networking technologies. Potential uses of AS/U for AIX include:

- Windows NT workstations in a Windows NT domain using an AIX server as a domain controller.
- A mixed workstation environment of UNIX and Windows NT with a single AIX server.

- Consolidating multiple Windows NT domains into a single larger domain using an RS/6000 SMP or SP system.
- Environments migrated to Windows NT requiring access to legacy UNIX systems.
- Windows NT servers and AIX servers in a single Windows NT domain.
- Multiple Windows NT domains on AIX servers using a partitioned RS/6000 SP.

6.2 Advanced Server for UNIX Installation

AS/U is delivered on one CD-ROM called "OpenTeam for AIX", which contains the product, NetBIOS for UNIX, additional filesets and documentation.

6.2.1 System Requirements

AS/U for AIX from Group Bull runs on most RS/6000 models, including all SMP and SP systems. Currently, OpenTeam is at Version 4.0. Prerequisites for AS/U are:

- AIX Version 4.1.1.2 or later (for our testing we used AIX 4.2.1). It is recommended by Bull that AIX is at Version 4.1.5 or that the following fixes, which are included in AIX 4.1.5, are installed:
  - U443437 - Base Operating System Multiprocessor runtime.
  - U443346 - Base Operating System TTY runtime.
  - U443440 - Front End Printer Support.
  - U445507 - Front End Printer Support (for non-purged printer queues).
- 64 megabytes of RAM.
- 110 megabytes of disk space.
- NetBIOS 3.0 for UNIX (this is included on the OpenTeam CD-ROM).

6.2.2 Filesets

The OpenTeam AS/U LPP for AIX has the following filesets:

asu.unix.devtk	AS/U development toolkit
asu.unix.man	AS/U manual pages
asu.unix.msclients	Microsoft Clients for AS/U
asu.unix.rpl	AS/U Remote Boot Service

asu.unix.server	AS/U
asu.unix.snmp	AS/U SNMP service
asu.unix.srvtools	Administrative tools for AS/U
ipf.dos.diskette	IPF (Install Package Facility) workstation diskette
ipf.dos.files	IPF files to install on workstation by OTSOFT
ipf.dos.samples	IPF samples to test installation on workstations
ipf.unix.admin	IPF package administration
netbios.kernel.diskette	NetBIOS for UNIX (DOS tools)
netbios.kernel.unix	NetBIOS for UNIX
snmp.dispatcher.daemon	SNMP dispatcher daemon
snmp.netbios.agent	SNMP agent for NetBIOS

The Install Package Facility cannot be used with Windows NT and will, therefore, not be discussed in this book.

6.2.3 Licensing

An iFOR/LS nodelock license is required for the OpenTeam software, AS/U and NetBIOS. A temporary key is supplied with the product and a permanent license will be supplied after registration. This is documented in the readme.wri file on the installation CD-ROM in the root directory.

6.2.4 Installing the CD-ROM

To install the OpenTeam CD-ROM (assuming that you do not already have a previous installation of LAN Manager for UNIX or AS/U), use `smit`:

1. Log in as root and type:
   `smit install_latest`
2. Press **F4** and select the CD-ROM drive from the list.
3. To install AS/U and NetBIOS for UNIX, leave the defaults on the installation screen (`_all_latest`) and press **Enter**.

6.2.5 Documentation

Documentation can be found on the OpenTeam CD-ROM. To access this information:

1. Insert the CD-ROM.

2. Mount the CD-ROM. To mount over /mnt:

```
mount -o ro -v cdrfs /dev/cd0 /mnt
```

The documentation is found in the doc directory on the CD-ROM. The documents supplied with OpenTeam 4.0, in Word for Windows and Postscript format, are:

c_p_40,conart40	Advanced Server Concepts and Planning Guide
admin40	Advanced Server Installation Guide
ipf	Install Package Facility
nbsetup	NetBIOS 3.0 Installation and Setup Guide
nbapi	NetBIOS 3.0 Programmer's Guide
nbsnmp	NetBIOS 3.0 SNMP Agent Reference Manual

On the OpenTeam CD-ROM (Version 4.0) that we used, there were two files in the root directory:

- readme.wri (information about the CD-ROM and installation)
- srb.wri (Bull Software Release Bulletin containing important information not found elsewhere in the documentation)

Both of these files are in the Windows Write format and have to be viewed with `write` or `wordpad` on a PC running a version of Windows.

6.2.6 Initial Setup

Once the OpenTeam products have been installed, AS/U can be configured with the simple setup. From a shell (on the server, not from a `telnet` session), type:

```
smit openteam_setup
```

Rather than take you to a SMIT panel, this will execute a script that takes you through a quick default setup of NetBIOS and AS/U. The script goes through the following steps (the choices we selected for our configuration are highlighted in bold):

1. NetBIOS configuration is started.
2. Choose the interface - **tr0**.
3. Configure TCP/IP or keep existing configuration - **keep**.
4. NetBIOS RFC 1001/1002 is started on lana0.
5. AS/U Configuration is started.

6. Choose the server name - **lv3010a_asu**.
7. Choose the role of the AS/U server (PDC or BDC) - **primary**.
8. Choose the domain name - **lv3010a_dom**.
9. Confirm the above choices - **y**.
10. Set the administrator password - **testasu**.
11. The AS/U setup completes the configuration and starts AS/U.

6.2.6.1 Tutorial

When the script has completed, NetBIOS and AS/U will have been started with the default configuration and parameters that were supplied. We recommend that, after this process, you run the AS/U tutorial. The tutorial can be run from SMIT:

```
smit advanced_server
```

Then select the **Advanced Server for UNIX Tutorial** menu item. The tutorial will let you read the latest readme file and also guide you through basic AS/U facilities.

6.2.6.2 AS/U Initial Setup Confirmation from AIX

When the AS/U and NetBIOS setup has completed, AS/U will be running. You can use the AS/U `net` command to see the current domain and computers belonging to it:

```
net computer
```

This will produce output similar to the following:

```
Advanced Server 4.0 for UNIX

These computers belong to domain lv3010a_dom:
Computer                 Type
-------------------------------------------
LV3010A_ASU              Primary
The command completed successfully.
```

You can also use the `net` command to see other domains:

```
net browser
```

If there other domains on the network, the command should produce output similar to the screen below:

```
Advanced Server 4.0 for UNIX

These domains are visible from your Domain Controller:
BAWLMER                 DOMAIN                  ITSOAUSNT
LV3010                  LV3010A_DOM             RTC
WG2630DO                WORKGROUP
The command completed successfully.
```

6.2.6.3 AS/U Initial Setup Confirmation from Windows

If you have an installed Windows NT system on the network, you can confirm that the AS/U installation was successful. If successful, you are able to see your new domain from other computers on the network.

From the Windows NT desktop, click on the **Network Neighborhood** icon, as shown in Figure 150.

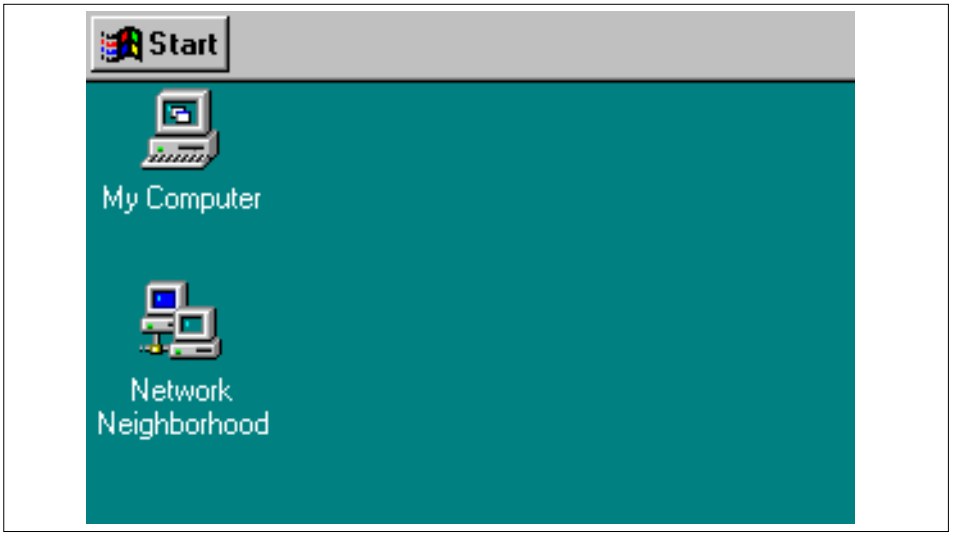


Figure 150. Network Neighborhood Icon

After clicking on the Network Neighborhood icon, a window will appear with a list of computers in the local domain/workgroup (as shown in Figure 151).

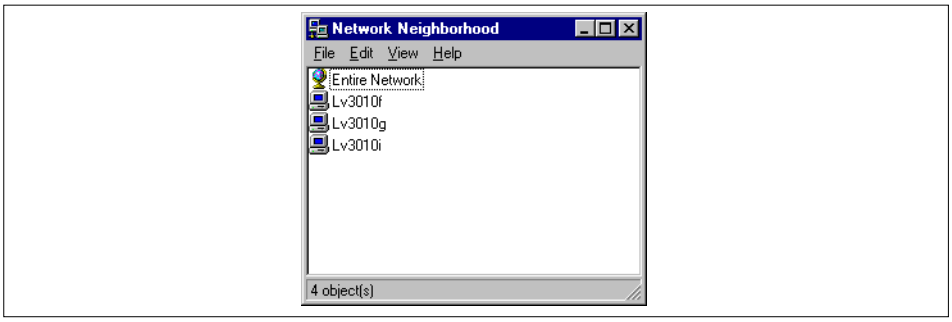


Figure 151. Network Neighborhood Window

Since the Windows NT system that we are using is not in the current AS/U domain (lv3010a_dom), we have to first click on **Entire Network**, and a window will appear (as shown in Figure 152). Then click on **Microsoft Windows Network**.

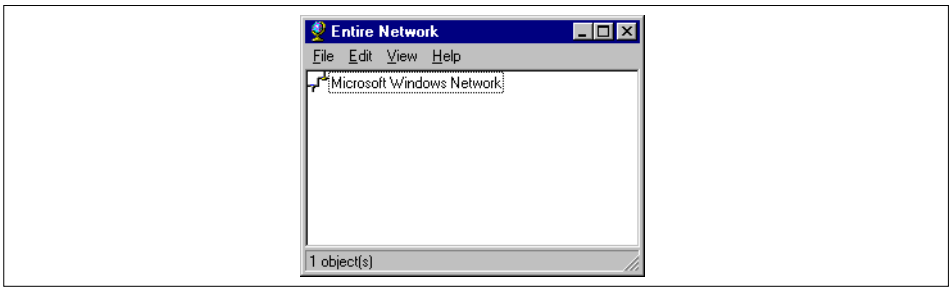


Figure 152. Network Neighborhood - Entire Network

Having clicked on the Microsoft Windows Network, another window will appear (as shown in Figure 153). In this window we can see all the domains and workgroups that are available. It is in this window that we can see our domain, lv3010a_dom. We can click on this domain and see a list of systems in the domain (as shown in Figure 154).

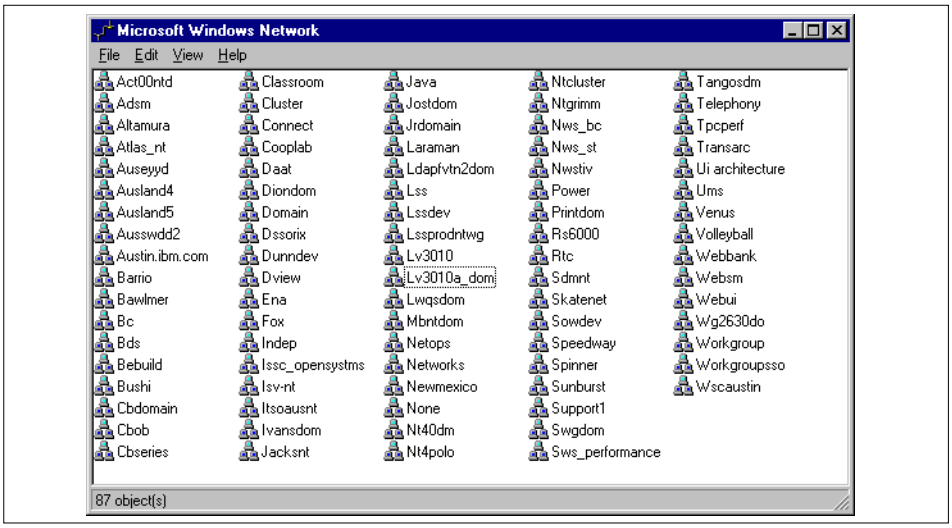


Figure 153. Microsoft Windows Network Systems

Since we have only configured the AS/U server, lv3010_asu, in the lv3010a_dom domain, this is the only system we can see (as shown in Figure 154).

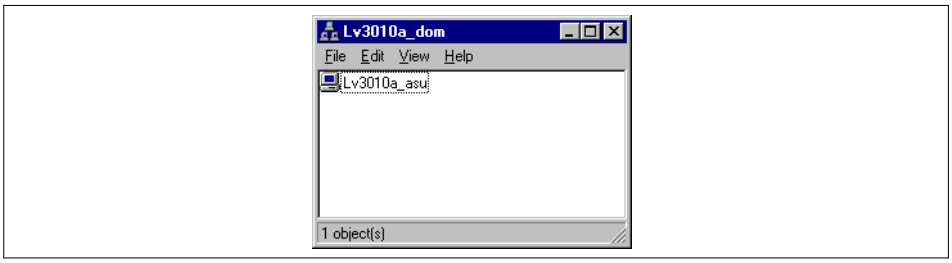


Figure 154. AS/U Lv3010_asu Domain

If we click on the lv3010a_asu system in the window, we are presented with a logon box as shown in Figure 155. Because we have a default account (userID - administrator and password tmpasu), we can log in to the AS/U server.

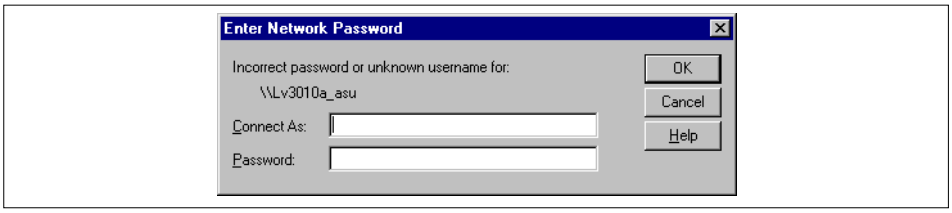


Figure 155. Network Logon

6.2.6.4 Viewing AS/U Resources

Having logged on to the AS/U server, we can now access the resources that are available. Figure 156 shows the resources that are available on lv3010a_asu.

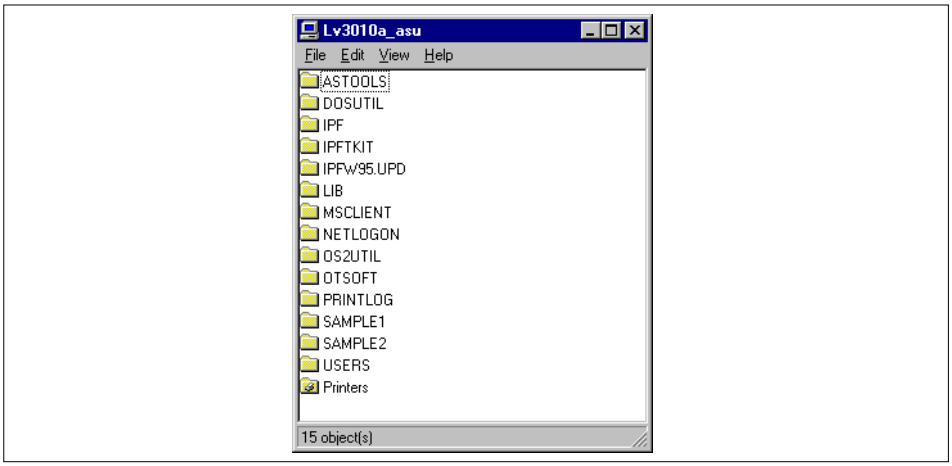


Figure 156. AS/U Resources

In Figure 156 we are shown a list of available volumes on the AS/U server. You can see which directories have been shared from the AS/U server with the `net share` command (entered on the RS/6000):

```
# net share
Advanced Server 4.0 for UNIX.

Share name   Resource                        Remark
------------------------------------------------------------------------------
ADMIN$       C:\HOME\LANMAN                  Admin Share
IPC$                                         IPC Share
C$           C:\                             Root Share
D$           C:\USR\NET\SERVERS\LANMAN\SH... SystemRoot Share
PRINT$       C:\USR\NET\SERVERS\LANMAN\SH... Printer Driver Share
ASTOOLS      C:\USR\NET\SERVERS\LANMAN\SH... Advanced Server Tools
DOSUTIL      C:\USR\NET\SERVERS\LANMAN\SH... DOS Utilities
IPF          C:\USR\OT\SOFT\IPF
IPFTKIT      C:\USR\OT\SOFT\IPFTKIT
IPFw95.UPD   C:\USR\OT\SOFT\IPFw95.UPD
LIB          C:\USR\NET\SERVERS\LANMAN\SH... Programming Aids
MSCLIENT     C:\USR\NET\SERVERS\LANMAN\SH... Microsoft Clients
NETLOGON     C:\USR\NET\SERVERS\LANMAN\SH... Logon Scripts Directory
OS2UTIL      C:\USR\NET\SERVERS\LANMAN\SH... OS/2 Utilities
OTSOFT       C:\USR\OT\SOFT
PRINTLOG     C:\USR\NET\SERVERS\LANMAN\SH... LP printer messages
SAMPLE1      C:\USR\OT\SOFT\SAMPLE1
SAMPLE2      C:\USR\OT\SOFT\SAMPLE2
USERS        C:\HOME                         Users Directory
The command completed successfully.
```

This shows you which directories have been shared, their path (the path will look like a PC path with the root being `c:` instead of `/` and the `\` symbols instead of `/` symbols) and any remarks that are available. Each of these represents a directory that has been defined on the AS/U server through the default setup. We can open these folders and their files from Windows NT (except for the special `$` directories).

6.3 Configuration

Now that we have connected to the RS/6000 and accessed the resources defined by the default setup, initial installation is complete. We can now proceed with the configuration of AS/U.

6.3.1 Adding a User

To add a user account to AS/U, we can use the `net` command:

```
net user test testpass /add
```

This adds a user with a user name of test and a password of testpass. This will not create a UNIX user. A UNIX user account can be manually matched to the user name or an AS/U registry change can be made (see 6.3.7, “AS/U

User Registry Settings” on page 206) so that the match occurs automatically when an AS/U user is created.

6.3.2 Changing a Windows NT Workstation Domain

Since this user has been created in our domain, we will be able to log on to workstations in our domain using the new user ID and password. In our test environment, we installed a Windows NT workstation that belongs to another domain. To be able to authenticate in our new AS/U domain we need to change the Windows NT workstation domain to lv3010a_dom. To do this, we have to log on to the Windows NT workstation as the administrator user. After logging on we have to change the domain:

1. Select the **Start Menu**.
2. Select **Settings**.
3. Select **Control Panel**.
4. Double-click on the **Network** icon.

This brings up the network window. The initial panel is the Identification panel. On this panel:

5. Select **Change**.

This displays the Identification Changes window (see Figure 157). It is here that we change the domain name to `lv3010a_dom`. We also have to specify an account on the AS/U server that has permission to add workstations to the domain. In our environment, only the administrator user with the password of testasuone has these permissions. Once we have filled- in the required fields we can click on **OK**.

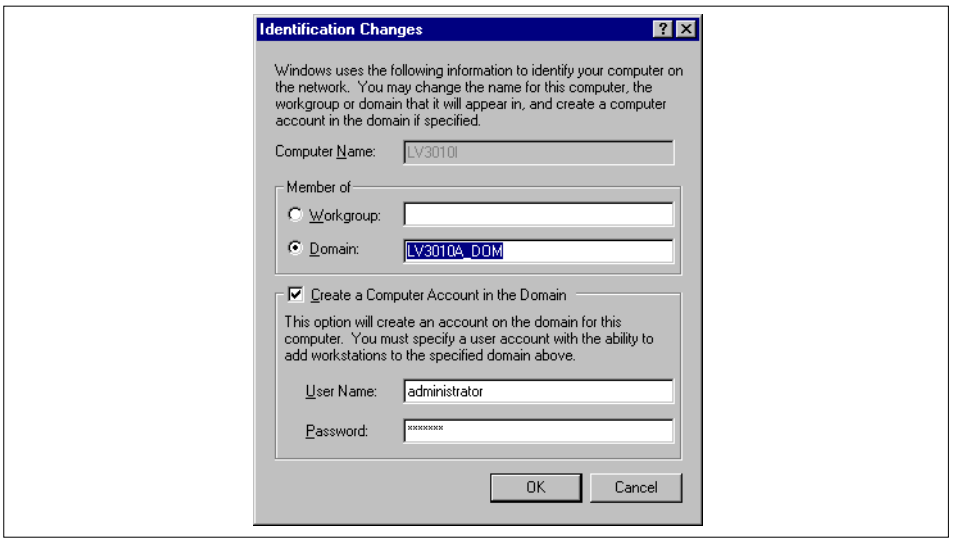


Figure 157. Windows NT Workstation Identification Changes

If the domain change is successful and the Windows NT workstation has joined the AS/U domain, a welcome window will appear (as shown in Figure 158).

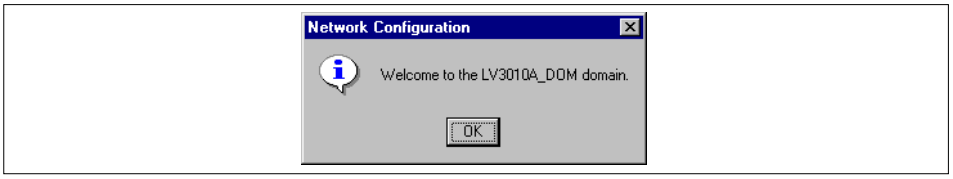


Figure 158. Domain Welcome Window

Once **OK** has been selected, a message will appear asking for the workstation to be rebooted.

After the workstation has been rebooted, we can use the `net` command on the RS/6000 to see that the workstation has joined the AS/U domain. To do so, type the following:

```
net computer
```

This produces a screen similar to the following:

```
Advanced Server 4.0 for UNIX.

These computers belong to domain lv3010a_dom:

Computer                Type
-------------------------------------------------------------------------------
LV3010A_ASU             Primary
LV3010I                 Workstation
The command completed successfully.
```

From the Windows NT workstation we can now see that the domain appears when the **Network Neighborhood** icon is clicked (without clicking on Entire Network), since the lv3010_dom is now our local domain (as shown in Figure 159).

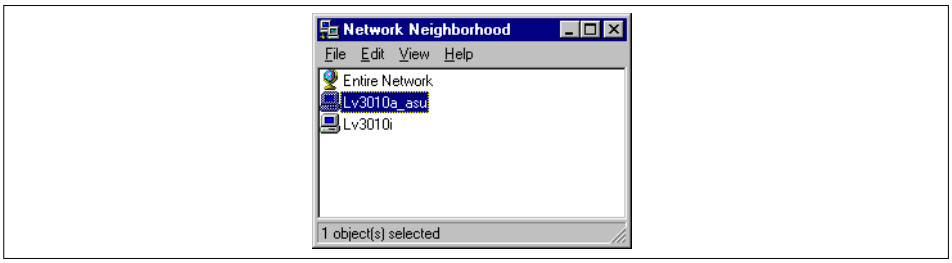


Figure 159. Network Neighborhood

6.3.3 Logging On to the AS/U Server

From the Windows NT workstation logon screen, we can log in locally to any account on the system or we can select the AS/U domain and log in with an account that has been set up on the RS/6000. Previously, we created a user, test, with password testpass. If we select lv3010a_dom, we can use this user ID to log on to the workstation (even though the account does not exist on the Windows NT workstation). If the user ID and password are entered correctly, this should log us onto the workstation. Once authentication has occurred, this presents a desktop for a new user. Since no configuration has been performed on the user test (in the lv3010a_dom domain on the AS/U server), the user profile will only be stored on the local Windows NT workstation in c:\winnt\profiles\test

This means that any changes the user makes to their desktop on the current workstation will stay on that workstation. If they logged on to the domain from another workstation, a new user profile would be created since the other system does not have access to the initial workstation. Moreover, since a

home directory has not been set up for the user, all files created by the user are stored on the local workstation and are not available on other systems. This situation is only useful when the user has a fixed workstation and authentication is required only at the server.

6.3.4 Configuring a User

In a previous example we used the `net` command to create the user test with a password testpass. With the `net` command we only set up the user name and password. However, there are several parts to a user account that can be set (examples of the `net` commands are given below the definitions):

User Name The unique user ID that the users type to log on.

Password The user's password.

Full Name The user's full name.

```
net user test /fullname:"Test User"
```

Description A description of the user account.

```
net user test /remark:"Test user on AS/U"
```

Logon Hours The hours during which the user can log on. The following example changes the users logon times to 8 a.m. to 6 p.m., Monday through Friday.

```
net user test /time:M-F,08:00-18:00
```

Logon Workstations By default, a user can log on from any workstation. If desired, this can be restricted to a list of workstations.

```
net user test /workstations:lv3010l
net user test /workstations:ALL
```

Expiration Date A date when the account will be disabled.

```
net user test /expires:12/31/98
```

Home Directory The user's home directory.

```
net user test /homedir:'\\lv3010a_asu\users\test'
```

Logon Script A batch file or executable file that automatically runs when the user logs on.

```
net user test /script:script.bat
```

Profile The path to a directory containing information about the user's desktop environment and settings.

```
net user test /profile:'\\lv3010a_asu\users\test'
```

Account Type Global or local accounts (default is global).

```
net user test /account:global
```

In addition, there are four conditions that can be set for each user account:

- User must change password at next logon (default is yes)
- User cannot change password (default is no)
- Password never expires (default is no)
- Account disabled (default is no)

All of the above parameters can be changed/set from the Windows NT Server using the User Manager for Domains (or from Windows NT after installing the AS/U client-based network administration tools).

6.3.4.1 Mapping an AS/U User to an AIX User

We would like to create an AIX user and directory so that when the user logs in from Windows NT, their home directory is the AIX file system and their profile is stored in the AIX home directory. For this example we create a user called fred by typing the following:

```
mkuser fred
```

This creates a user, fred, with a home directory /home/fred. We can then create a profile directory in this home directory for the Windows NT profile settings by typing the following:

```
mkdir /home/fred/ntprofile
```

This will not have the correct ownership (unless it was created by the user fred), so we can change this:

```
chown fred:staff /home/fred/ntprofile
```

It is a good idea to set the permissions for read, write and execute only for fred, and read only for others in the staff group. To do so, enter the following:

```
chmod 750 /home/fred
chmod 750 /home/fred/ntprofile
```

For the AS/U user fred to access the directory /home/fred, the user directory needs to be shared. We may add other users, so instead of sharing each user's directory individually, we can share just the /home directory:

```
net share home=c:/home /remark:"AIX users directory"
```

We can create and configure the AS/U user fred with one or more `net` commands. In the current release of AS/U, however, we found that you are forced to use one `net` command to create a user and specify all the options.

When we tried to use net commands to add or modify options for users we created, we found that the user could not log into the AS/U server.

To create the AS/U user fred with a password of fredpass, we can use the net command. The following net command sets the profile directory of the AS/U user fred to the ntprofile directory in the AIX user fred home directory that we created. It also sets fred's AS/U home directory to the AIX user fred home directory. In addition, the /fullname option specifies the full name of the AS/U user fred and the /remark option specifies a description of the user:

```
net user fred fredpass /add /profile:'\\lv3010a_asu\home\fred\ntprofile' \
/homedir:'\\lv3010a_asu\home\fred' /remark:"User Fred on ASU" \
/fullname:"Fred User"
```

We can now map the AS/U user fred to the UNIX user fred using the mapuname command (the command may not be in the root path, it can be found in /usr/net/servers/lanman/bin):

```
mapuname -a LV3010A_DOM:fred fred
```

Now, any files created on the AS/U server by the AS/U user fred will be owned by the AIX user fred.

All the user information for the AS/U fred user can be viewed with the net command:

```
# net user fred
Advanced Server 4.0 for UNIX.
User name                    fred
Full Name                    Fred User
Comment                      User Fred on ASU
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never
Account type                 Global

Password last set            01/28/98 03:03 PM
Password expires             03/11/98 03:03 PM
Password changeable          01/28/98 03:03 PM
Password required            Yes
User may change password     Yes
User must change password     No

Workstations allowed         All
Logon script
User profile                 \\lv3010a_asu\home\fred\ntprofile
Home directory               \\lv3010a_asu\home\fred
Last logon                   Never

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users
Primary Group                *Domain Users
The command completed successfully.
```

We can also use the `net` command to view the shared directories to check that the home directory is shared:

```
# net share
Advanced Server 4.0 for UNIX.

Share name   Resource                        Remark
------------------------------------------------------------------------------
ADMIN$       C:\HOME\LANMAN                  Admin Share
IPC$                                         IPC Share
C$           C:\                             Root Share
D$           C:\USR\NET\SERVERS\LANMAN\SH... SystemRoot Share
PRINT$       C:\USR\NET\SERVERS\LANMAN\SH... Printer Driver Share
ASTOOLS      C:\USR\NET\SERVERS\LANMAN\SH... Advanced Server Tools
DOSUTIL      C:\USR\NET\SERVERS\LANMAN\SH... DOS Utilities
HOME         C:\HOME                         AIX users directory
IPF          C:\USR\OT\SOFT\IPF
IPFTKIT      C:\USR\OT\SOFT\IPFTKIT
IPFW95.UPD   C:\USR\OT\SOFT\IPFW95.UPD
LIB          C:\USR\NET\SERVERS\LANMAN\SH... Programming Aids
MSCLIENT     C:\USR\NET\SERVERS\LANMAN\SH... Microsoft Clients
NETLOGON     C:\USR\NET\SERVERS\LANMAN\SH... Logon Scripts Directory
OS2UTIL      C:\USR\NET\SERVERS\LANMAN\SH... OS/2 Utilities
OTSOFT       C:\USR\OT\SOFT
PRINTLOG     C:\USR\NET\SERVERS\LANMAN\SH... LP printer messages
SAMPLE1      C:\USR\OT\SOFT\SAMPLE1
SAMPLE2      C:\USR\OT\SOFT\SAMPLE2
USERS        C:\HOME\LANMAN                  Users Directory
The command completed successfully.
```

Now that the user fred has been created and configured, we can try to log onto the Windows NT workstation that we added to our domain. If we select `lv3010a_dom` at the dialog box, we can use the AS/U user fred to log onto the workstation. If everything has been successful, the user fred will see the Windows NT Welcome window and a new desktop. A shared drive will be available.

While the user fred is logged into the Windows NT workstation, a profile directory is used on the local system, c:\winnt\profiles\fred (it is created if it does not exist). If a profile for fred exists on the AS/U server, the local profile will be a copy of this. Any changes that fred makes to his profile during his session are copied to the AS/U server when fred logs out.

6.3.5 Installing AS/U Server Tools

Using a Windows NT server or workstation system, you can administer your AS/U server. This includes creating and maintaining users on the AS/U system. Windows NT Workstation, however, does not come with the tools required to perform the administration. These tools come with AS/U and can be copied and installed onto the local Windows NT workstation. To install the tools:

1. Click on the **Network Neighborhood** icon on the desktop.
2. Click on the **lv3010a_asu** system.
3. Log in as the administrator.
4. Copy the **ASTOOLS** directory to the local Windows NT workstation.
5. Run the **setup** program in the astools\asuadm directory.
6. Run the **setup** program in the astools\english\winnt directory.

After running both of the setup scripts, the following programs are installed in the c:\winnt\system32 directory on the Windows NT workstation:

- **asuadm.exe** - AS/U Administrator Tool
- **poledit.exe** - Policy Editor
- **usrmgr.exe** - User Manager
- **srvmgr.exe** - Server Manager
- **winsadmn.exe** - WINS Manager

6.3.6 Using AS/U Server Tools

The AS/U Administrator allows you to edit specific AS/U parameters that are stored in the AS/U registry (such as whether a UNIX system account is generated when an AS/U account is generated).

To be able to use the AS/U administration tools, the local Windows NT system has to be logged onto the AS/U server. To do this, open the **Network Neighborhood** and click on the **lv3010a_dom** system. This will present a dialog box. Log on as the administrator.

6.3.6.1 User Manager

You can start the User Manager program from within the AS/U administrator tool or by clicking on its icon. Once loaded, it presents a window as shown in Figure 160.

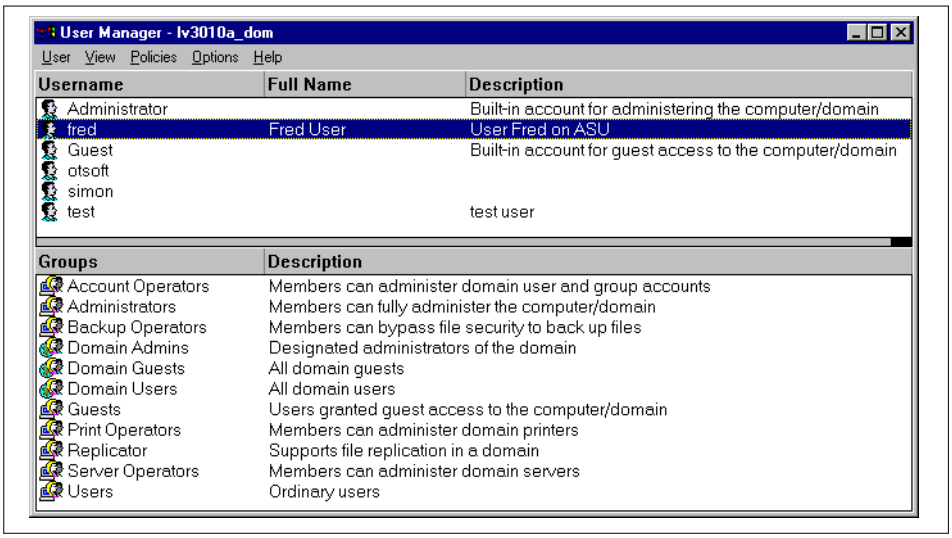


Figure 160. Windows NT User Manager

If the User Manager program is started directly, it will only show the local users. To administer the AS/U users:

1. Select **User** menu.
2. Select **Select Domain** menu.

This will present a window (as shown in Figure 161). Double-clicking on the **lv3010_dom** domain displays a list of users configured on our AS/U server (as shown in Figure 160).

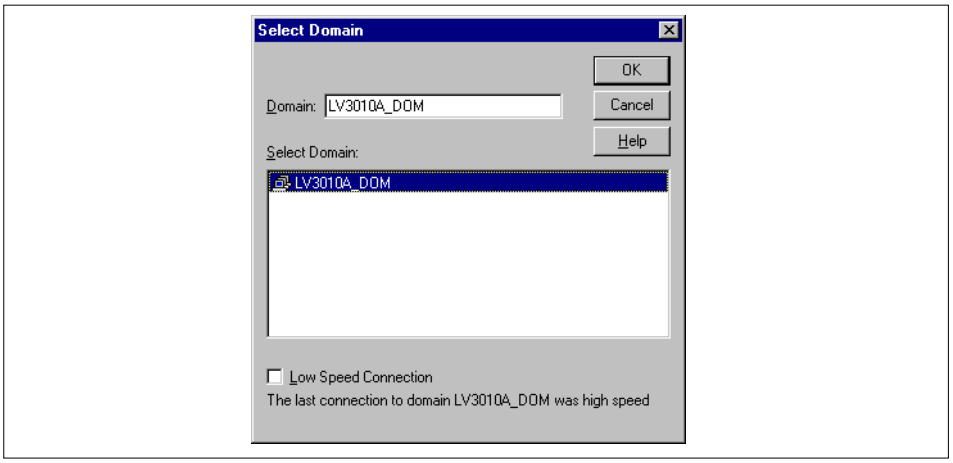


Figure 161. Select Domain

We can see that the AS/U user fred, that we created on the RS/6000 with the `net` command, is visible. Clicking on the user fred presents us with a window where we can change the user attributes. The initial window, as shown in Figure 162, gives us details about the user ID, user name, password and logon options.

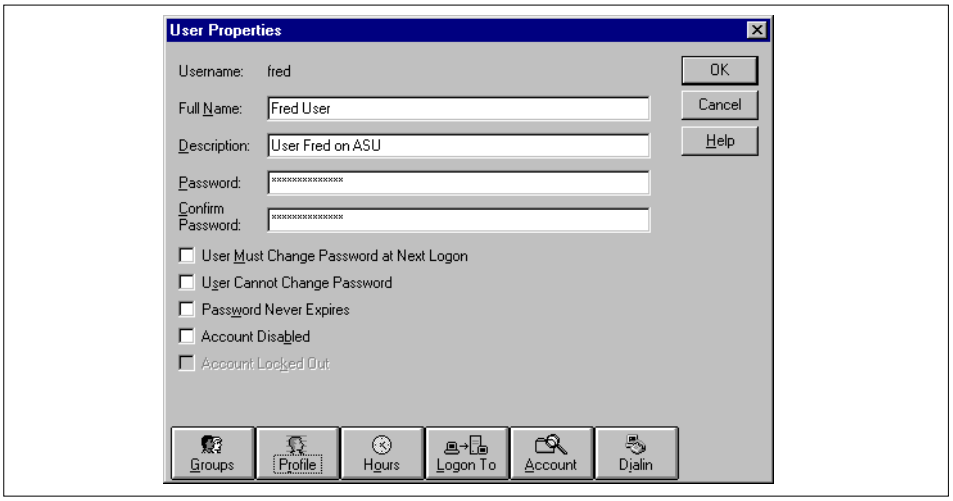


Figure 162. Window User Properties

Clicking on **Profile** produces a window, as shown in Figure 163, where the path of the profile and home directories can be set. As shown in the example,

the lv3010a_asu server has been set for both, and the home directory has been given a default mapping to the Z: drive. On the AS/U server, only /home has been set up as a shared directory (not /home/fred), so the Z: mapping will be to /home on the AIX system, not /home/fred. The /home/fred home directory will become the default directory for the user fred (which will become z:\fred on the Windows NT system). If the user fred opens a DOS window, the directory will be /home/fred on the AIX AS/U server. Certain programs will also default the path for the save as option to the /home/fred AIX directory.

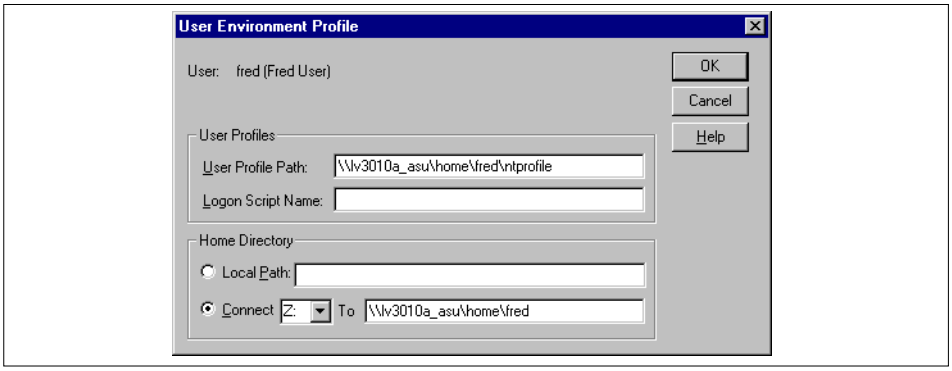


Figure 163. User Profile Settings

With the user manager we can add users or make further modifications to existing users. These users will be created on the AS/U server.

6.3.7 AS/U User Registry Settings

With our example user, fred, we manually created an AIX account and mapped the AS/U user fred to the AIX account. We can change the way AS/U works by enabling AS/U to create an AIX account automatically when an AS/U user is created. The change is made by editing the AS/U registry. Editing the registry can be easily performed from a Windows NT system (with the Windows NT `c:\winnt\system32\regedit32` program). You can also edit the AS/U registry directly on the AS/U AIX server. The `regconfig` command is used make changes to the registry.

There are three values that are of interest. The first two are in the UserServiceParameters registry entries. These are the CreateUnixUser and NewUSerShell registry settings in the HKEY_LOCAL_MACHINE key. The CreateUnixUser registry setting has to be set to `1` to enable an AIX account to be created automatically. The command to run is:

```
regconfig \
```

```
SYSTEM/CurrentControlSet/Services/AdvancedServer/UserServiceParameters \
CreateUnixUser REG_DWORD 1
```

By default, when AS/U creates the AIX user, it sets the users login shell to /bin/false. If you want the AIX user to be able to login, you must set this to a real shell. The command to set this to /usr/bin/ksh is:

```
regconfig \
SYSTEM/CurrentControlSet/Services/AdvancedServer/UserServiceParameters \
NewUserShell REG_SZ /usr/bin/ksh
```

Registry keys can be displayed with the `regconfig` command. For the two keys that were changed with the previous commands:

```
# regconfig -v SYSTEM/CurrentControlSet/Services/AdvancedServer\
/UserServiceParameters

KeyName SYSTEM\CurrentControlSet\Services\AdvancedServer\UserServiceParameters
ClassName
NumberOfSubkeys         0
LengthLongestSubkeyName 0
LengthSecurityDescriptor 240
MaxValueNameLength      26
MaxValueDataLength      60
LastWriteTime           Thu Jan 29 10:44:29 1998
CreateUnixUser:REG_DWORD:1
Exclude:REG_SZ:0-100
ForceUniqueUnixUserAccount:REG_DWORD:0
GroupUpdateTime:REG_DWORD:3600
NewUserShell:REG_SZ:/usr/bin/ksh
SyncUnixHomeDirectory:REG_DWORD:0
UserComment:REG_SZ:Advanced Server for UNIX user
UserRemark:REG_SZ:Users Directory
```

The third registry setting of interest is in the LanmanServer\Parameters registry entries. The UserPath registry setting is where the path for the AIX user is specified. By default, AS/U sets the AIX user's home directory to /home/lanman. We can change this to the regular /home directory, as shown below:

```
regconfig SYSTEM/CurrentControlSet/Services/LanmanServer/Parameters \
UserPath REG_SZ 'c:\home'
```

Again, we can use the `regconfig` command to confirm that this entry was entered correctly:

```
# regconfig -v SYSTEM/CurrentControlSet/Services/LanmanServer/Parameters
KeyName                 SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
ClassName               GenericClass
NumberOfSubkeys         0
LengthLongestSubkeyName 0
LengthSecurityDescriptor 240
MaxValueNameLength      14
MaxValueDataLength      66
LastWriteTime           Thu Jan 29 10:53:41 1998
AccessAlert:REG_DWORD:5
AutoDisconnect:REG_DWORD:0
ErrorAlert:REG_DWORD:5
Hidden:REG_DWORD:0
LmAnnounce:REG_DWORD:0
LogonAlert:REG_DWORD:5
SrvAnnounce:REG_DWORD:180
SrvComment:REG_SZ:Advanced Server for UNIX Systems
UserPath:REG_SZ:c:\home
```

For the registry changes to become effective, AS/U will have to be stopped and restarted.

After restarting AS/U, adding an AS/U user will create an AIX user:

```
net user jane jane /add /profile:'\\lv3010a_asu\home\jane\ntprofile' \
/homedir:'\\lv3010a_asu\home\jane' /fullname:"Jane User"
```

This will not, however, create the home directory or the profile directory. To create these and set the correct permissions, type the following:

```
mkdir -p /home/jane/ntprofile
chmod 750 /home/jane /home/jane/ntprofile
chown jane:staff /home/jane /home/jane/ntprofile
```

AS/U does not assign a password to the AIX user. This can be set by root or when the user first logs on (at the first login, the user will not be asked for an existing password but will be prompted to supply a new password).

It is useful to create a small script to automate the process of creating a user with a small number of input parameters.

6.4 Printers

Potentially, one of the most important components of AS/U is print serving. From AS/U, both local and remote printers can be shared with clients.

6.4.1 Configuring Printers

Provided that printers have already been configured to AIX, they can easily be shared by AS/U with the `net` command. For example, if we have a printer queue on AIX called final, and we wish to share the printer as lvfinal, we can share this printer with the following command:

```
net share lvfinal=final /print
```

This will create an AS/U queue for the AIX printer final. To use the printer, however, Windows NT users will have to install a printer driver for the printer from their installation CD-ROM.

6.4.1.1 AS/U Printer Installation from Windows NT

AS/U allows automatic downloading of print drivers for Windows NT clients. For this to occur, the printer has to be set up from Windows NT. In this section we describe printer setup using Windows NT.

On our server, lv3010a_asu, we have a print queue, final, that we want to share with the Windows NT clients. The printer is a Lexmark Optra N and is not local to the AS/U server:

```
# lpstat -pfinal
Queue   Dev   Status    Job Files            User       PP   %  Blks  Cp  Rnk
------- ----- --------- --- ---------------- ---------- ---- -- ----- --- ---
final   @prt3 READY
final   final READY
final   i0@to READY
```

To install this printer on the AS/U server (for use in Windows NT), log onto a Windows NT workstation and perform the following steps:

1. Click on the **Network Neighborhood** icon.
2. Click on **lv3010_asu**.
3. Click on **Printers**.
4. Click on **Add Printer**.

This will present a window (see Figure 164) asking you to install a remote printer on the AS/U server (lv3010a_asu in our example). Click **Next** to continue:

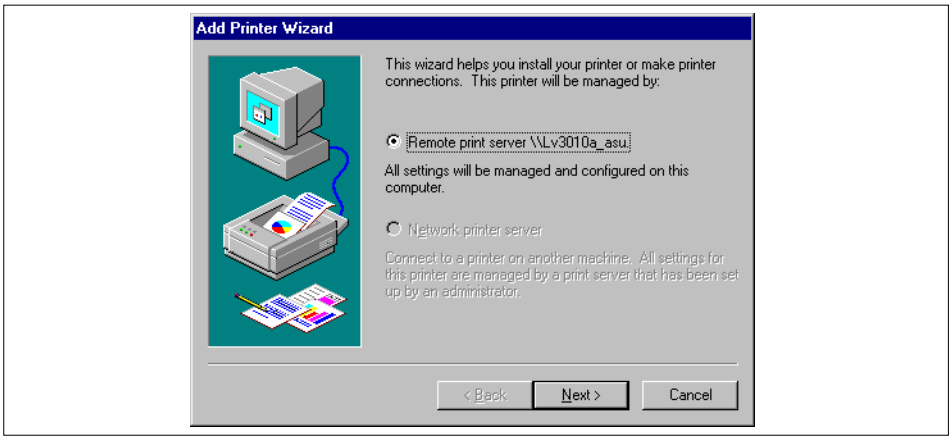


Figure 164. Add Printer Wizard

After clicking **Next** (see Figure 164), we are presented with a list of printers that are available on the AS/U server (see Figure 165). This list includes the final printer queue that we want to add. First, we put a check mark next to the final queue and then click on **Next**.

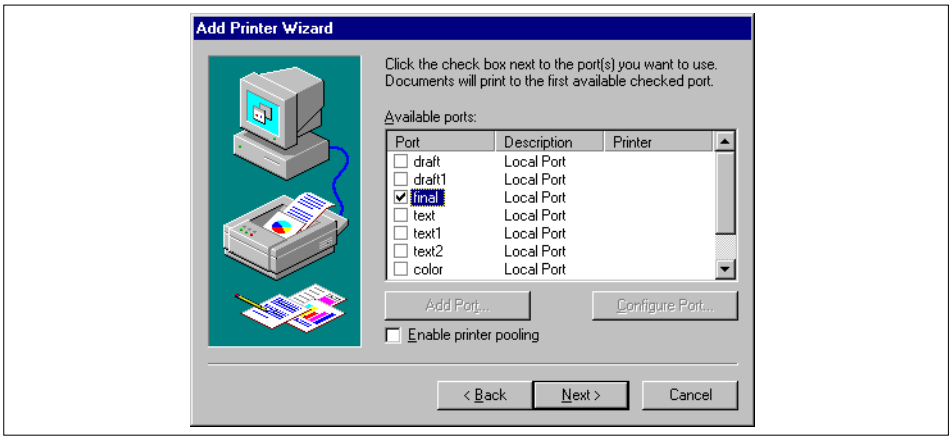


Figure 165. Selecting AS/U Print Queue

Windows NT then asks for the printer manufacturer and model. A large list is presented. In our example, we are adding the Lexmark Optra N PS (see Figure 166). After selecting the correct printer driver, click **Next**.

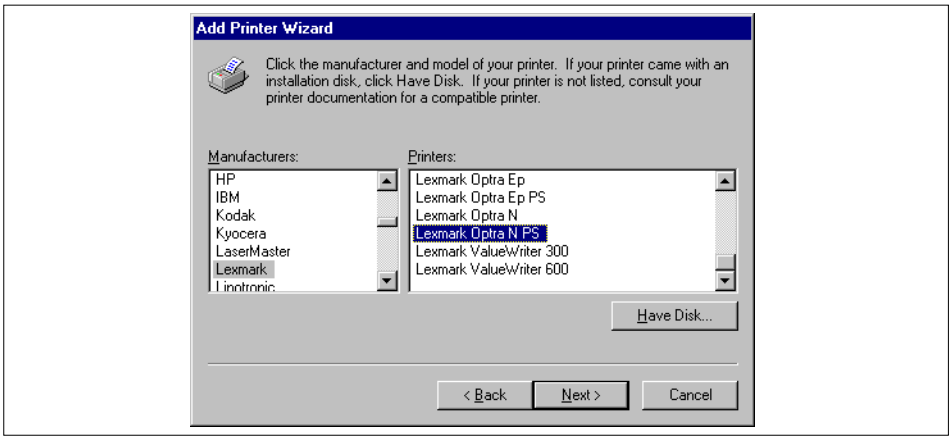


Figure 166. Selecting Printer Type

Windows NT then asks for the name of the printer (this can be any name, although we found that Windows NT would not allow it to be the same name as the RS/6000 queue name). In this example, we call it Optra (see Figure 167).

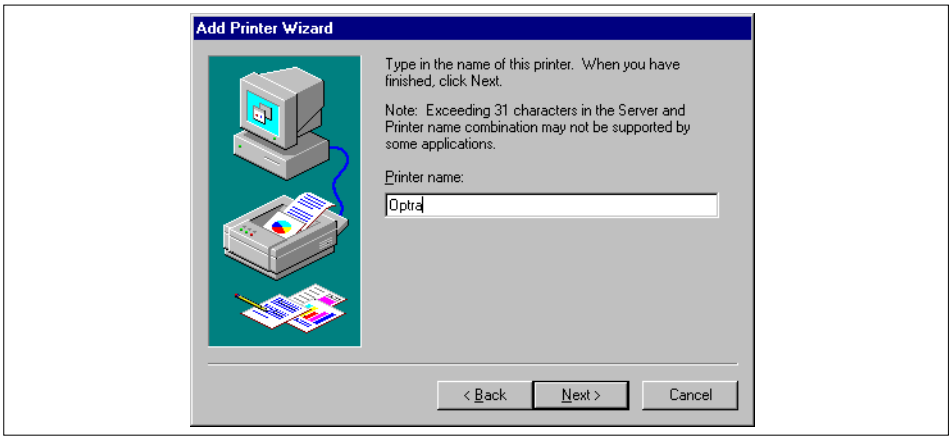


Figure 167. Choosing Printer Name

After clicking **Next**, Windows NT asks if the printer is to be shared (Figure 168). Once the shared item has been selected, the share name has to be entered. At this point, you can install printer drivers for other platforms with which the printer could be shared. Since we are only using Windows NT 4.0, no other drivers are selected.

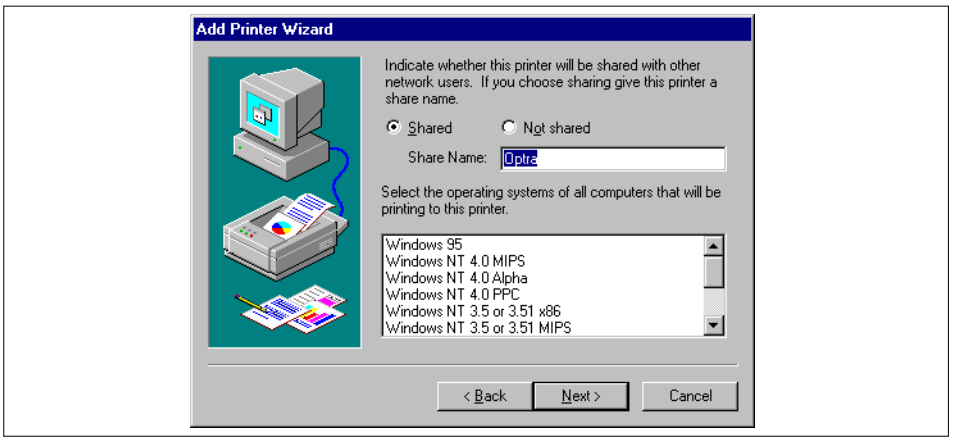


Figure 168. Sharing the Printer

After clicking next, Windows NT asks if a test page should be printed. If the printer is correctly installed on the RS/6000, this should be performed. Clicking on **Finish** completes the installation. Windows NT will now install the driver for the printer from the Windows NT installation CD-ROM and copy them to the AS/U server so that other systems can have the printer drivers installed automatically.

After the installation has completed, clicking on the **lv3010a_asu** system in the network neighborhood should show the printer in the list of resources (Figure 169).

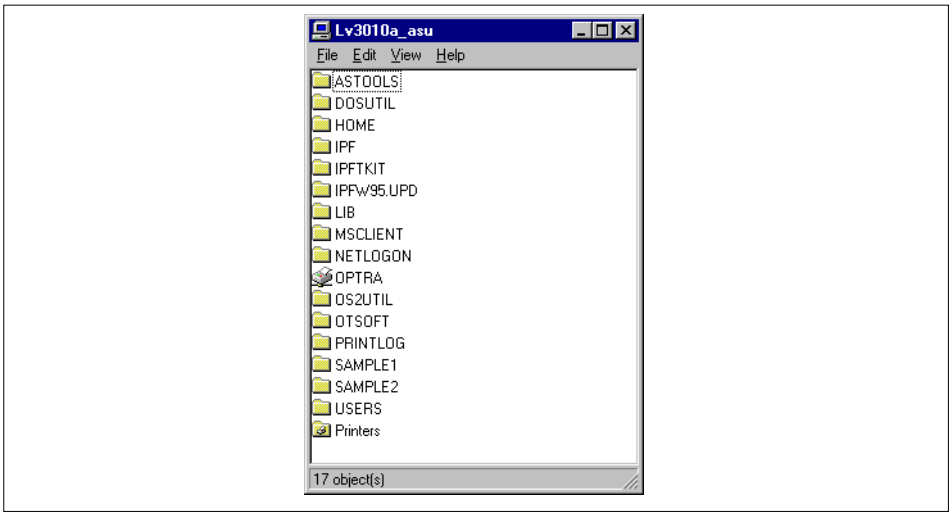


Figure 169. AS/U Server Resources

6.4.1.2 Installing an AS/U Printer on Windows NT

The printer will not have been set up on the local Windows NT system. You can now have the printer automatically installed on the local and other Windows NT systems by bringing up the AS/U server resources window (as shown in Figure 169) and clicking on the Optra printer icon. This presents a window (see Figure 170) that asks if you want to set the printer on the current system. Selecting **Yes** will automatically install the drivers for the printer from the AS/U server. If no current printer is installed on the Windows NT system, it will be set up as the default printer.

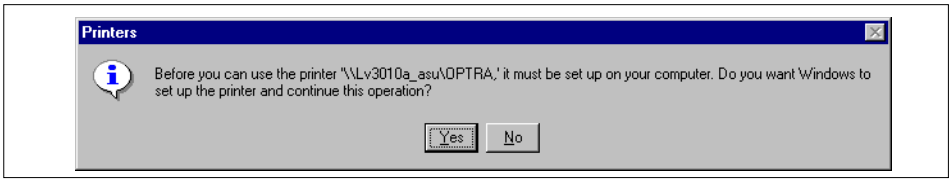


Figure 170. Installing a Windows NT Printer from an AS/U Server

Each individual user will have to go through this process. The printer installation will only be available to users who install the printer.

On the AS/U server, you can look at the printers that are configured and view any jobs that are in the queues with the following command:

```
net print
```

If a print job is currently printing from the Windows NT workstation, you can use this command to look at the progress of the job, as shown below:

```
# net print
Advanced Server 4.0 for UNIX.

Printers at LV3010A_ASU

Name                         Job #      Size            Status
------------------------------------------------------------------------------
OPTRA Queue                1 jobs                      *Printer Active*
     ADMINISTRATOR           1004     44019           Printing
The command completed successfully.
```

6.4.2 Setting Up Printer Queues with Different Priority Levels

Windows NT and AS/U print queues can be configured with different priorities. This is useful if you have more than one print queue pointed to a particular printer on the server. Using print priorities, two or more print queues can be set up so important jobs will print before unimportant jobs. This means that important jobs that are queued after the unimportant jobs will still print first.

6.4.2.1 Installing a Second Printer Queue

In 6.4.1.1, “AS/U Printer Installation from Windows NT” on page 209, we configured an AS/U printer queue called Optra. To add a second queue, follow the same steps (using the same print queue, final on the RS/6000) but call the printer Optra2 (or any unique name). To add the printer, ensure that you are logged on as administrator in the AS/U domain. Once the printer has been installed, add this to the local Windows NT system (as described in 6.4.1.2, “Installing an AS/U Printer on Windows NT” on page 213).

6.4.2.2 Changing the Queue Priorities

Now that two printer queues have been added to the AS/U server, we can set the priority of each queue. In our example we want the Optra2 queue to have a lower print priority than the Optra queue. To do this, we will leave the Optra queue with its default priority of 85 and reduce the priority of the Optra2 queue.

To change the priority of a print queue:

1. From the Windows NT desktop select **Start**.
2. Select **Settings**.
3. Select **Printers**.

4. Highlight **Optra** or **Optra2**.
5. Select **File** Menu.
6. Select the **Priorities** menu item.
7. Select **Scheduling**.
8. Drag the Priority slider to the desired priority.

In our example we reduce the priority of the Optra2 queue (as shown in Figure 171) to 70.

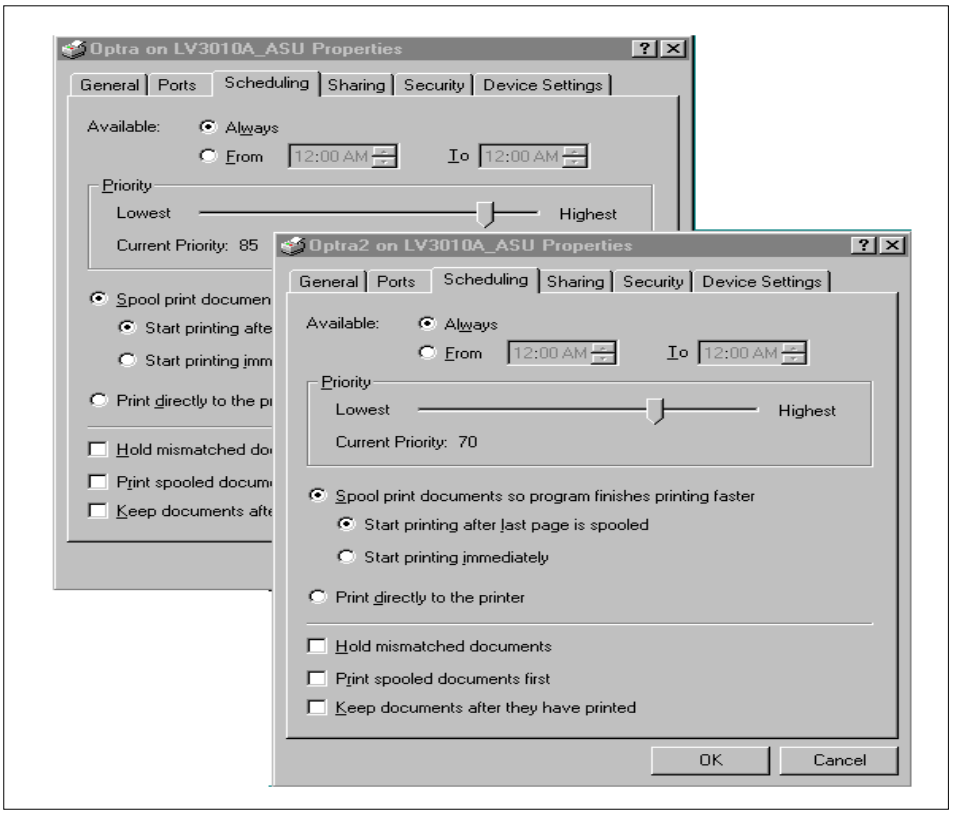


Figure 171. Setting Printer Queue Priorities

Now that the Optra2 queue has a lower print priority, any jobs submitted will be sent to the print after the optra queue is cleared.

Now that we have two printer queues, we can actually control access to the different queues, enabling two different sets of users to access the printer

with different priorities. This is described in 6.5.3, “Creating Groups to Control a Resource” on page 218.

6.4.3 Setting Up a Printer Pool

AS/U supports printer pooling where two or more printers can be associated with a single print queue. This is useful if you have a lot of printing and want to distribute the workload automatically between several printers. All the printers must be the same hardware model, but can be connected through the network in parallel or serially.

A printer pool determines which printer is idle and sends the job to that printer. If a printer stops printing, all other jobs are sent to other devices in the pool. The current print job will resume when the printer is back online.

In addition to being part of a printer pool, a printer can have its own print queue so that jobs can be directed straight to a particular printer.

6.4.3.1 Installing a Pooled Print Queue

In 6.4.1.1, “AS/U Printer Installation from Windows NT” on page 209, we configured an AS/U printer queue called Optra. To set up a queue that uses a printer pool, follow the same steps but on the port selection window, select **Enable Print Pooling** and then one or more RS/6000 printers. In our example we have two identical printers called draft and draft1 (see Figure 172). To add the printer, ensure that you are logged on as administrator in the AS/U domain. Once the printer has been installed, add this to the local Windows NT system (as described in 6.4.1.2, “Installing an AS/U Printer on Windows NT” on page 213).

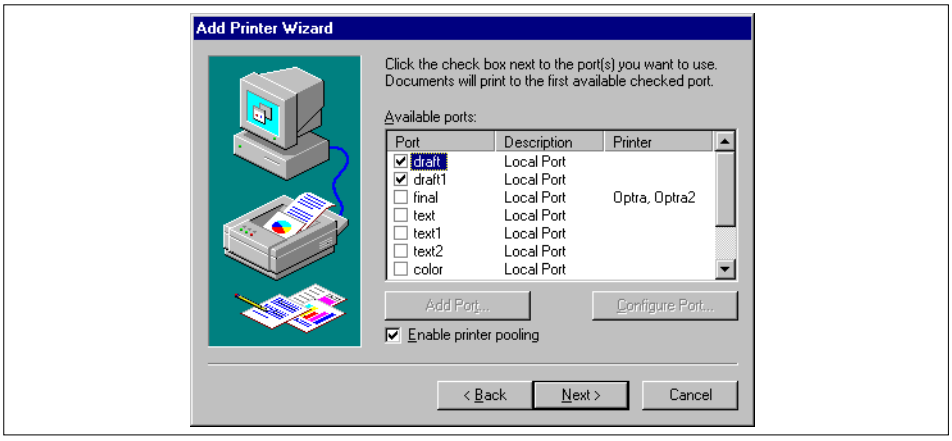


Figure 172. Print Pooling

Now that the printer has been set up on the AS/U server, other Windows NT systems can access the printer pool as one queue.

6.5 Groups

Windows NT and AS/U, like AIX, allow the use of groups. Groups allow collections and rights and capabilities to be assigned to users. There are two types of groups that can be configured:

Global groups A global group contains a number of user accounts from one domain. In addition, a global group is able to receive rights and permissions in multiple domains. Global groups can be added to local groups in the same domain, domains that trust the domain or to member servers or computers running Windows NT in the same or trusting domain.

Local groups A local group contains user accounts and global accounts from one or more domains. Local groups can only receive permissions and rights in a single domain.

6.5.1 Global Groups

Global groups that are currently configured on the AS/U server can be viewed with the `net` command:

```
# net groups
Advanced Server 4.0 for UNIX.

Group Accounts for \\LV3010A_ASU
-------------------------------------------------------------------------------
*Domain Admins            *Domain Guests            *Domain Users
The command completed successfully.
```

Members of a particular group can be viewed with the `net` command:

```
# net group 'domain admins'
Advanced Server 4.0 for UNIX.
Group name     Domain Admins
Comment        Designated administrators of the domain

Members
-------------------------------------------------------------------------------
Administrator
The command completed successfully.
#
# net groups 'domain users'
Advanced Server 4.0 for UNIX.
Group name     Domain Users
Comment        All domain users

Members
-------------------------------------------------------------------------------
Administrator            fred                    Ian
jane                     LV3010$                 LV3010A_ASU$
LV3010H$                 LV3010I$                LV3010K$
otsoft                   simon                   test
The command completed successfully.
```

6.5.2 Local Groups

Local groups that are currently configured on the AS/U server can also be viewed with the `net` command:

```
# net localgroup
Advanced Server 4.0 for UNIX.

Aliases for \\LV3010A_ASU

-------------------------------------------------------------------------------
*Account Operators       *Administrators          *Backup Operators
*Guests                  *Print Operators         *Replicator
*Server Operators        *Users
The command completed successfully.
```

6.5.3 Creating Groups to Control a Resource

We currently have a printer defined on the AS/U server, called Optra, and we only want to be able to let certain users use the printer. The following steps enable a number of users to use this printer:

1. Create a global group for users to have permission to print to the optra printer:

   ```
   net group printgrp /add
   ```

2. Add to the global group the users that want to be able to print to the printer.

   ```
   net group printgrp test jane fred /add
   ```

3. Create a local group that will have permission to print to the Optra printer:

   ```
   net localgroup printlocal /add
   ```

4. Add the global group to the local group:

   ```
   net localgroup printlocal printgrp /add
   ```

By default, the printer queue Optra was created with print permission for everyone. To allow only users in our printgrp to access the Optra printer, we need to remove the everyone group from the printer. To configure the permissions we must perform the following steps:

1. Log on to a Windows NT system as the administrator in the lv3010a_dom domain.
2. Open the AS/U server from within the Network Neighborhood.
3. Click on the **Optra** printer icon. If the printer has not already been installed on the current Windows NT system, then let AS/U install the printer.
4. Select the **Printer** menu.
5. Select the **Properties** menu item.
6. Select the **Security** tab.
7. Click on **Permissions**. A window appears, as shown in Figure 173.

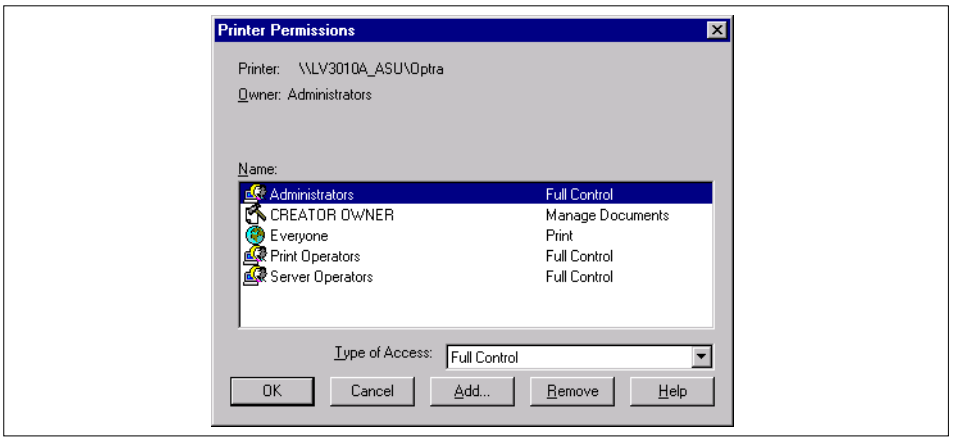


Figure 173. Printer Permissions

8. Click on the **Everyone** icon.

9. Click **Remove**.

10. Click on **Add**.

11. Click on the **Printlocal** group (see Figure 174).

12. Select **Print** as type of access.

13. Click on **Add** (see Figure 174).

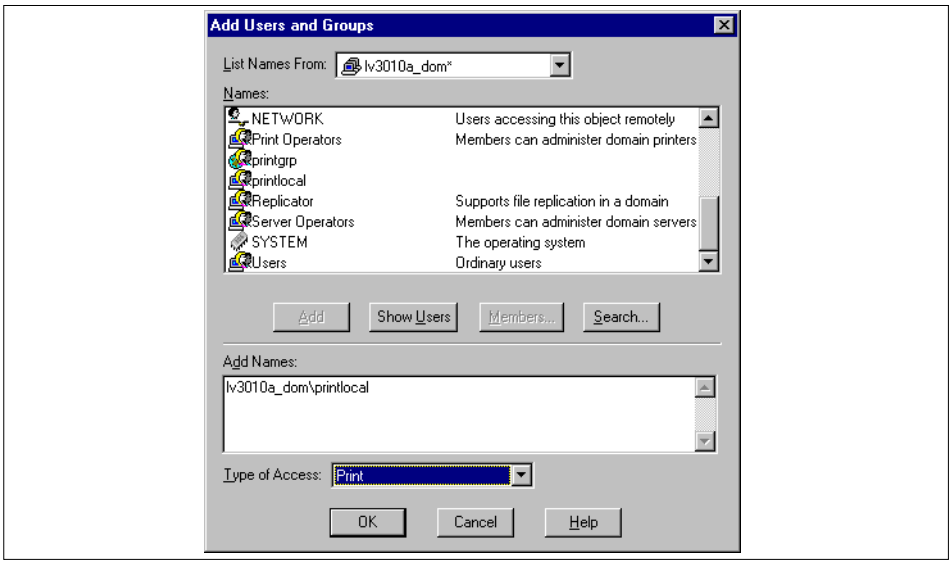


Figure 174. Printer - Add Users and Groups

14. Click on **OK**.

The printer permissions window will now display the new printlocal group added with print permission (see Figure 175). Click on **OK** to complete the operation.

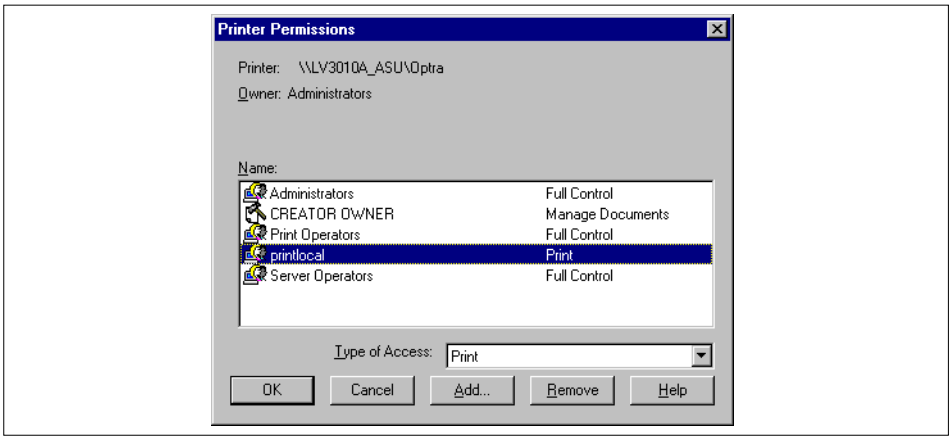


Figure 175. Print Permissions with New Printlocal Group

Users in the printgrp group are now able to access the printer on the AS/U server. Any user (without explicit permission to use the printer such as the administrator) who is not in the printgrp group will be presented with an access denied message (see Figure 176).

Figure 176. Printer Connection Denied Message

6.6 File and Directory Security

The use of groups in AS/U allows users to be granted or denied access to resources, such as printers and directories. AS/U also allows file and directory permissions that specify which users have access and at what level that access is permitted. The permissions are provided on two levels:

Share permissions Defines the access for users and groups on files and directories belonging to the share.

Directory access permissions Defines access for users and groups on particular files and directories.

6.6.1 Share Permissions

Share permissions allow users to share resources and files. For instance, we have several documents we want to share with a set of users configured in AS/U (fred, ian and jane). The documents are in a file system on AIX with a path of /docs. The first step is to change the permissions and ownership for the directory so AS/U users have access to the directory (using the default lmxadmin user and DOS---- group):

```
chmod 775 /docs
chown lmxadmin:DOS---- /docs
```

We can then share this directory with our clients:

```
net share documents=c:/docs /remark:"Important Documents"
```

By default, the directory is associated with the group everyone. We can remove the everyone group and add the users we want to access the shared directory by using the Server Manager program from Windows NT (permissions can be manipulated by AS/U, but we found that this gave unstable results). To remove the everyone group and allow users fred, ian and jane to access our newly-created share documents from a Windows NT system, perform the following steps:

1. Log on to the AS/U server as **administrator**.
2. Start the server manager program - **srvmgr**.
3. Select the **Computer** menu.
4. Select the **Select Domain** menu item.
5. Select AS/U domain - **lv3010a_dom**.
6. Highlight AS/U server - **lv3010a_asu**.
7. Select the **Computer** menu.
8. Select the **Shared Directories** menu item. A window appears, as shown in Figure 177.

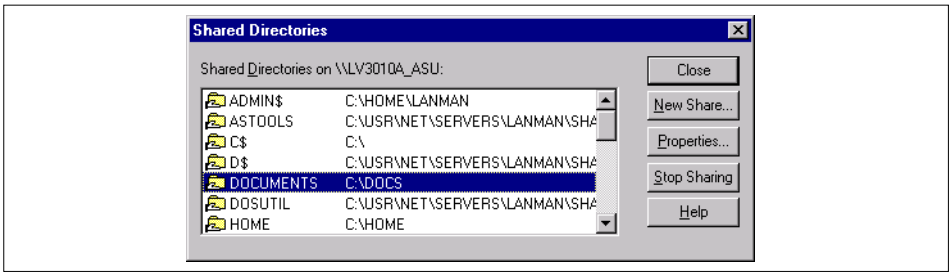


Figure 177. Shared Directories

9. Highlight the **DOCUMENTS** directory.
10. Click **Properties**. A window appears (see Figure 178) showing information about the shared directory. If you want to restrict the number of users who can concurrently use the shared directory, use this window to configure it. To do this, select the **Allow** option under User Limit and specify how many users you want to able to access the directory concurrently.

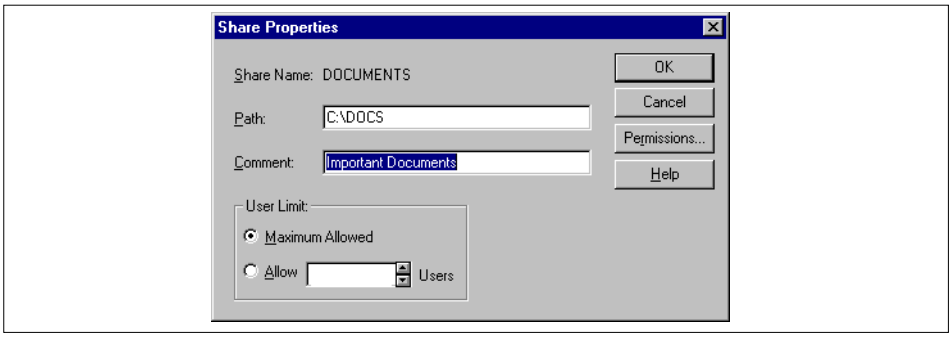


Figure 178. Share Properties

11. Click **Permissions** and a window is displayed (see Figure 179). In this window you can see that the group everyone has full control of this shared directory.

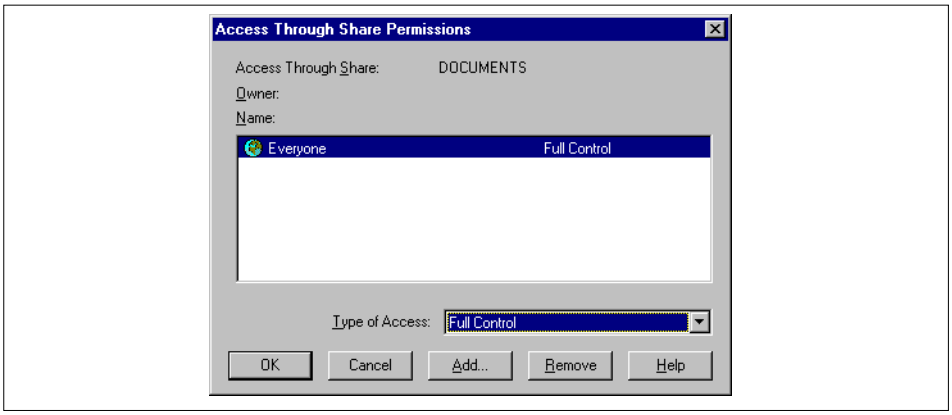


Figure 179. Share Access Permissions

12.Highlight the **Everyone** group.

13.Click on **Remove**.

We now want to configure the users fred, ian and jane to have full access to this directory:

14.Click on **Add.** A window with a list of groups appears (see Figure 180).

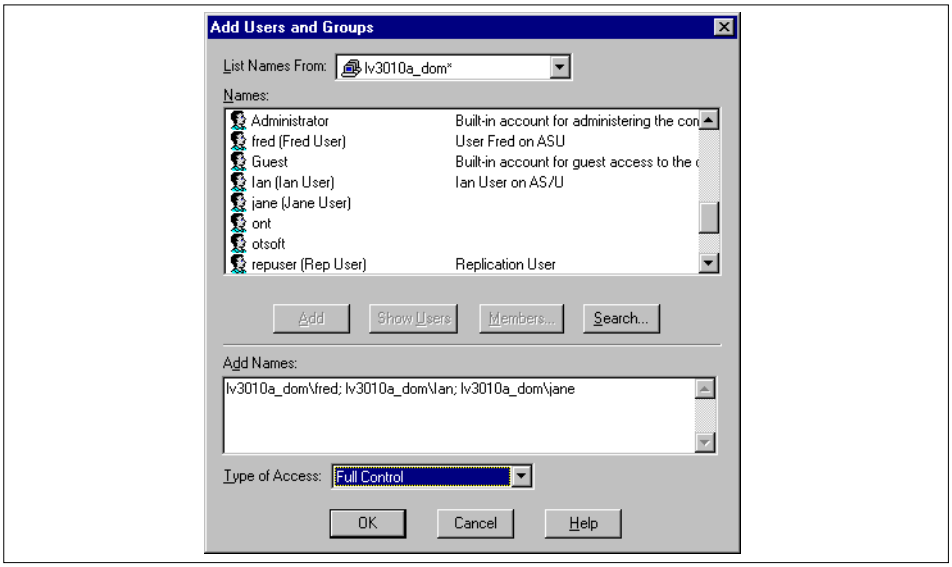


Figure 180. Add Users and Groups

15. Click on **Show Users**.
16. Double-click **fred**, **jane** and **ian**.
17. Under Type of Access, select **Full Control.** The window should look like the one shown in Figure 180.
18. Click on **OK**. The permissions window (see Figure 181) now shows that only fred, jane and ian have permissions for the shared directory and that they all have full control (they can create, remove, add files and so forth).

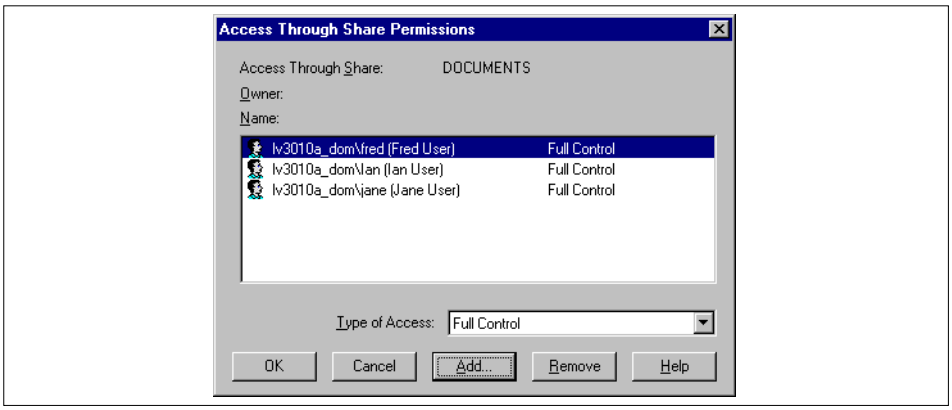


Figure 181. Share Access Permissions

19. Click on **OK**.
20. Click on **OK**.
21. Click on **Close**.
22. Exit from the srvgmgr program.

6.6.2 Directory Permissions

In 6.6.1, “Share Permissions” on page 222, we configured the permissions for an individual share. In our example we have a directory full of documents (/docs on the AS/U server). As this directory has been currently configured, fred, ian and jane can create and remove any documents in this directory. We may want, however, to have directories belonging to each of the users in this directory where the files can be read by everyone but only deleted or changed by their owner.

Jane has a directory in /docs directory called jane. By performing the following she can change the permissions on this directory so that only she can remove or change files, but fred and ian have read access:

1. Log in to the AS/U server from Windows NT as jane.
2. Open the **documents** share folder.
3. Right-click on folder **jane**.
4. Select **Security**.
5. Click **Permissions** (see Figure 182).

Included in the permissions for jane's document directory is the group everyone, with full access control. In this instance, it means that users ian and fred can access jane's directory (other users can't access the directory because they do not have access to the share documents folder). If you only want ian and fred to have read access to jane's documents, you can easily change the everyone group to have read access only. Alternatively, you can add the individual users ian and fred with read access only to the permissions for the directory.

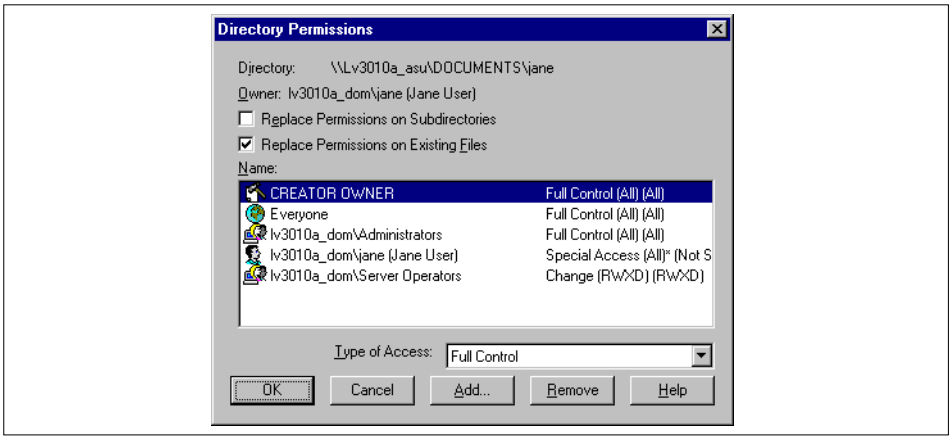


Figure 182. Directory Permissions for User Jane

In our example we will modify the everyone group:

6. Highlight the **Everyone** group (from Figure 182).
7. Select the **Read** option from Type of Access.
8. Click on **OK**.
9. Click on **OK**.

Now jane will have full access to her own directory but ian and fred will only be able to read files in the directory, not modify or delete them.

6.6.3 File Permissions

To edit permissions on individual files, follow the same procedure as described for 6.6.2, “Directory Permissions” on page 225, but instead of selecting a directory, select a directory and follow the instructions to modify the permissions.

6.7 Adding a Backup Domain Controller to the AS/U Domain

Now that a fully working AS/U server is up and running we can add a backup domain controller to our domain. This allows the domain to be more robust and also reduces the demands on our PDC. User accounts and profiles that are stored in the Security Accounts Manager (SAM) database on the PDC can automatically be replicated to the BDC. The PDC and BDC can then share authentication of client logons.

6.7.1 Windows NT Server as the Backup Domain Controller

We could add another RS/6000 running AS/U or a Windows NT Server as the BDC. In our test environment, we added a Windows NT Server as the BDC. To set up a Windows NT Server as a BDC to our AS/U Server, we perform the following steps:

1. Start installing Windows NT Server.
2. The installation asks for details about the computer name and the domain to which it is being adding. For our example, our responses are in bold:

   Computer Name - **lv3010h**

   Domain - **lv3010a_dom**

   Administrator Name - **administrator**

   Password - **testasu**

After entering the details, the system finishes the installation. During the completion of the installation, the Windows NT Server system replicates information from the AS/U server (including user account information). After the replication has occurred and the system has restarted we can log in to the system as the administrator on the AS/U server.

6.7.1.1 Confirming the Backup Domain Controller Installation

We can confirm that the new Windows NT Server system we have installed is part of the lv3010a_dom domain by running the `net` command on the AS/U server:

```
# net computer
Advanced Server 4.0 for UNIX.
These computers belong to domain lv3010a_dom:

Computer                Type
-------------------------------------------------------------------------------
LV3010A_ASU             Primary
LV3010H                 Backup
LV3010I                 Workstation
The command completed successfully.
```

In the output from the `net` command we can see that the new Windows NT server lv3010h is now seen as the BDC from AS/U.

6.7.1.2 Domain Replication

Any changes that are made on the AS/U server will now be replicated to the Windows NT Server BDC. If we make a change to the domain (adding a user for example), we can look at the event viewer on Windows NT BDC to see that a replication has occurred. To start the event viewer, select **Start** from the task bar, select **Programs**, select **Administrative Tools** and then **Event Viewer**. If we add a user, after replication the event viewer will show that a netlogon event has occurred (see Figure 183).

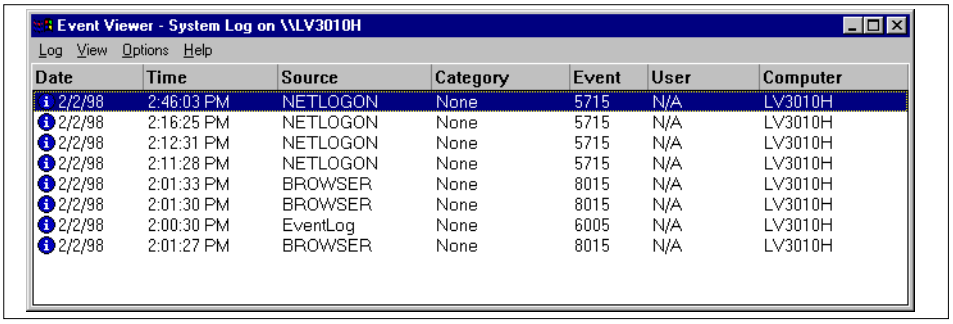


Figure 183. Event Viewer - System Events Output

The top event shows the replication event that occurred. If we click on this event, we are presented with details about the replication (see Figure 184).

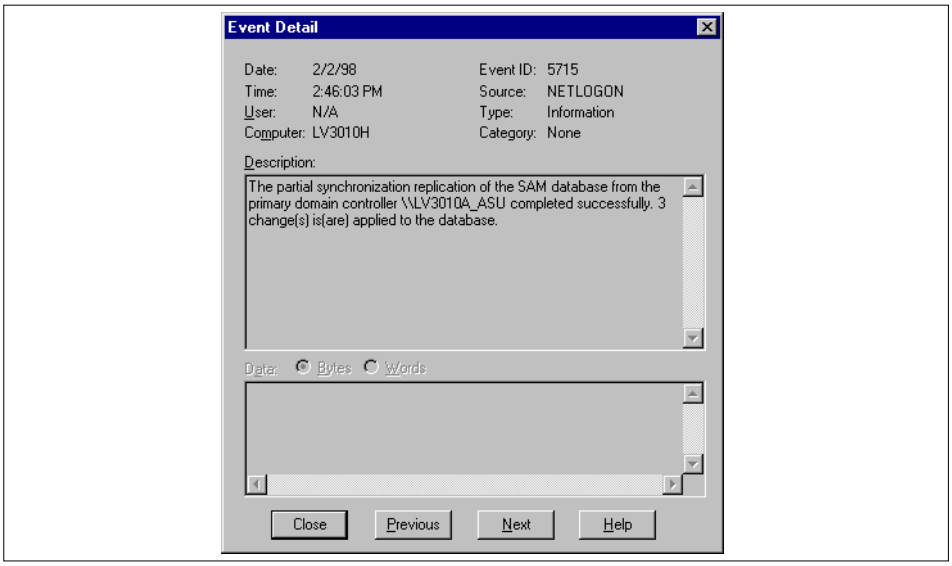


Figure 184. SAM Replication Event Detail

We can see that the SAM database was partially replicated from the PDC. It was partially replicated, because only information that has been updated since the last replication is copied from the PDC.

The following is a list of changes that can be made to the directory database:

- New passwords or changed passwords
- New or changed user accounts
- New or changed group accounts
- Changes in group memberships
- Changes in user rights

These changes are stored in the change log on the server. The PDC will contact the BDC to request an update of the database approximately every five minutes. The change log can store approximately 2000 changes. If there are more than 2000 changes between updates, the BDC will request a full copy of the database. If there are multiple BDCs, the updates will be staggered so that there is not a flood of activity going on at any one time. The update interval can be changed by editing the AS/U registry net logon service parameters. The item that sets this interval is the pulse parameter. The valid parameters are 60 to 3600 (one minute to one hour). If we want to change the

interval updates to 600 seconds (10 minutes) from the default setting of five minutes, we use the following `regconfig` command:

```
regconfig SYSTEM/CurrentControlSet/Services/Netlogon/Parameters \
Pulse REG_DWORD 600
```

We can view the netlogon registry settings with the `regconfig` command (including the changed pulse parameter):

```
# regconfig  -v SYSTEM/CurrentControlSet/Services/netlogon/parameters
KeyName                 SYSTEM\CurrentControlSet\Services\netlogon\parameters
ClassName
NumberOfSubkeys         0
LengthLongestSubkeyName 0
LengthSecurityDescriptor 240
MaxValueNameLength      12
MaxValueDataLength      134
LastWriteTime           Wed Feb  4 13:48:17 1998
LogonQuery:REG_DWORD:900
Pulse:REG_DWORD:600
QueryDelay:REG_DWORD:2
Randomize:REG_DWORD:30
RelogonDelay:REG_DWORD:2
Scripts:REG_EXPAND_SZ:%SystemRoot%\usr\net\servers\
                                        lanman\shares\asu\repl\export\scripts
SSIPasswdAge:REG_DWORD:604800
```

If a change has been made to the database and a copy is required immediately on the BDC, the update can be forced. This can be performed from a Windows NT system. We can either synchronize the entire domain or synchronize with the primary domain controller. Both of these options can be performed from the Windows NT server or a Windows NT system with the AS/U server tools. To do this we must first:

1. Start **Server Manager**.
2. Select the **Computer** menu.
3. Select the **Select Domain** menu item.
4. Select **lv3010a_dom**.

The first option, Synchronize Entire Domain, copies the latest directory database changes to all BDCs in the domain. To do this, perform the following steps:

1. Select the **Computer** menu.
2. Select the **Synchronize Entire Domain** menu item.
3. Server Manager asks for confirmation, select **Yes**.

4. An information message is displayed, click on **OK**.

The second option, Synchronize with Primary Domain Controller, copies the latest directory database changes to a selected BDC in the domain. If we want to update the lv3010h Windows NT system, which is our BDC, we can perform the following from within the server manager:

1. Click on the **lv3010h** item.
2. Select the **Computer** menu.
3. Select the **Synchronize with Primary Domain Controller** item.
4. Server Manager asks for confirmation, select **Yes**.
5. An information message is displayed, click on **OK**.

Both of the synchronizations can be checked by using the Windows NT Event Viewer to see that the updates have occurred.

If we shut down the AS/U server (the PDC) the BDC (lv3010h, a Windows NT Server system) will be used for authentication of users within the lv3010a_dom domain. With the PDC shut down, a user from within the domain can still log into a workstation in the domain, but when they do, a message appears stating that their roaming profile is not available. If they have previously logged onto the Windows NT Workstation they will be given the opportunity to use the local profile stored on the system. Any changes made to their profile while they are logged in with the PDC not running will be stored locally. If the user logs out and the PDC is brought back online before they log into the same workstation, the user is asked if they want to use the local profile, since it is more current than the one stored on the AS/U server. When they log out, the profile is copied to the AS/U server.

If the AS/U server (the PDC) is not running, users are authenticated through the BDC, but no changes to users can be made until the PDC is back online. Running the User Manager program on the BDC results in a message stating that the PDC is not available.

6.8 Directory Replication

AS/U supports the Windows NT service of directory replication (called the directory replicator service). Directory replication is useful for automatically distributing sets of files to one or more systems. Windows NT servers and AS/U servers can be export servers (where the original files are stored) or import servers (where the files are replicated to). Windows NT workstations can only be import servers.

Import servers replicate all the directories an export server has. An import server cannot specify which ones to import.

Typically, a server will use the directory replicator to replicate user logon scripts to the BDC, enabling workload to be distributed among domain controllers. However, any directory containing files can be replicated.

6.8.1 Replication Setup

By default, the AS/U server has the directory /var/opt/lanman/shares/asu/repl/export as the default export path. All directories that are replicated are subdirectories of the export path. You can export as many subdirectories of the export path as you like.

In the following example, we create a directory called test under the export path containing two files, testfile1 and testfile2:

```
cd /var/opt/lanman/shares/asu/repl/export
mkdir test
echo "Text for testfile1" > test/testfile1
echo "Text for testfile2" > test/testfile2
```

Before we configure directory replication, a user account to use for the replication must be added. If we create this user from Windows NT, we must deselect `User must change password at next logon` and select `Password never expires`. To create a user for replication (repuser) in the domain (lv3010a_dom in our example), enter the following:

```
net user repuser reppasswd /add /fullname:"Replication User" \
/comment:"Replication User" /passwordmustchg:no /passwordexp:no
```

6.8.1.1 Configuring Replication Export Server

To configure the directory replication service on the AS/U server (lv3010a_asu in our example), perform the following steps:

1. Log on as **administrator** in lv3010a_dom to a Windows NT Server or Workstation with the AS/U server tools.
2. Start the **Server Manager** program by entering `srvmgr`.
3. Select the **Computer** menu.
4. Select the **Select Domain** menu item.
5. Select **lv3010a_dom** domain.
6. Highlight **lv3010a_asu** system.
7. Select the **Computer** menu.

8. Select the **Services** menu item.
9. Select **Directory** Replicator.
10. Click on **Startup** and a window appears, as shown in Figure 185.
11. Select **Automatic**.
12. Select **This Account**.
13. Fill in user account- **lv3010a_dom\repuser**.
14. Fill in password - **reppasswd**.

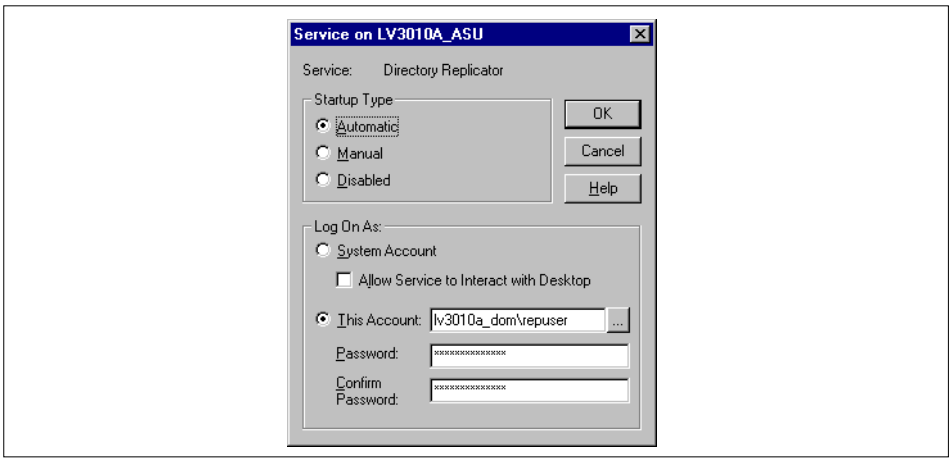


Figure 185. Directory Replicator Service Details

15. Click on **OK**.
16. An information message appears, telling you that the repuser has been configured correctly (see Figure 186).

Figure 186. Directory Replicator Information Message

17. Click on **OK**.
18. Select **Close** to complete.

6.8.1.2 Configuring Replicator Export Directory

Now that the service has been configured, the export directory can be added to the replicator service:

1. From within the server manager program highlight **lv3010a_asu**.
2. Click **Replication**.
3. Select **Export Directories** (this will select our default export path on the AS/U server - lv3010a_asu), see Figure 187.

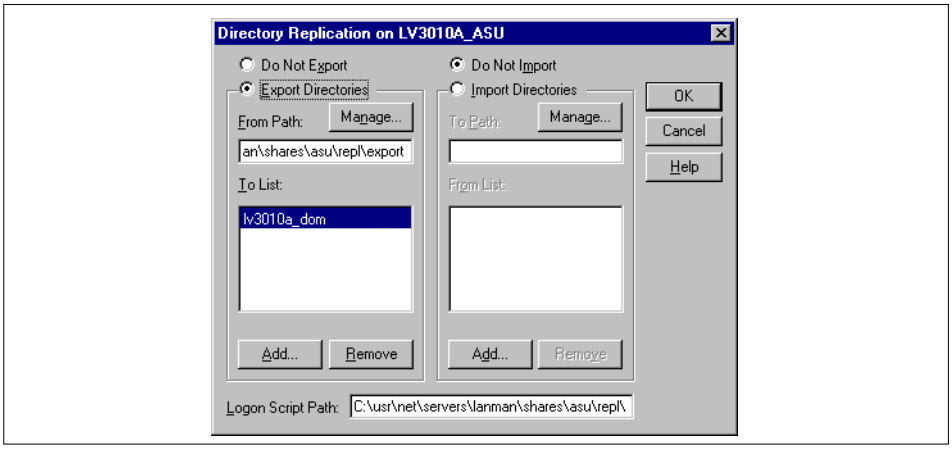


Figure 187. Selecting Directory Replication Export Directory

4. Click on **Manage** (Under Export Directories).
5. Click on **Add**.
6. Type **test** (for our test directory).
7. Click on **OK**.
8. The test directory is shown (see Figure 188).

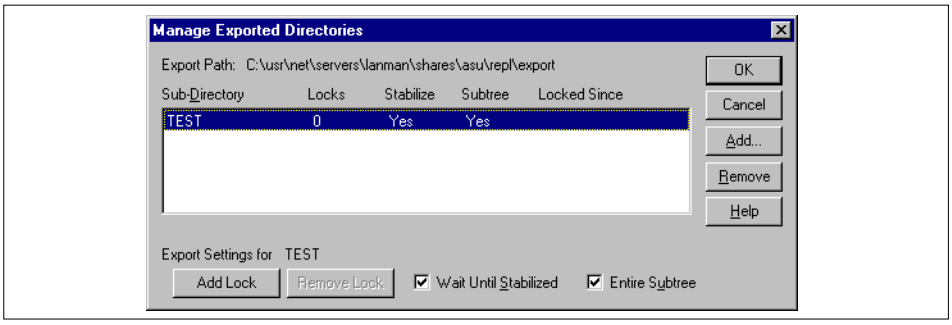


Figure 188. Manage Export Directories

9. Click on **OK**.
10. Click on **OK**.
11. The directory replication is started.
12. Click on **OK**.

6.8.1.3 Configuring Import Server

The AS/U server is now configured as the export server. We can now configure an import system. In our network, we have a Windows NT workstation in the lv3010a_dom domain to which we want to replicate the test directory. To configure the Windows NT workstation as an import computer, perform the following steps:

1. Start the **Services** program in the control panel.
2. Highlight **Directory Replicator**.
3. Click on **Startup**.
4. Select **Automatic**.
5. Enter **lv3010a_dom\repuser** for the user.
6. Enter the password - **reppasswd**.
7. Click on **OK**.
8. An information message appears, click on **OK**.
9. Start the **Server** program in the control panel.
10. Click on **Replication**.
11. Select **Import** - this will use the default path of c:\winnt\system32\repl\import.

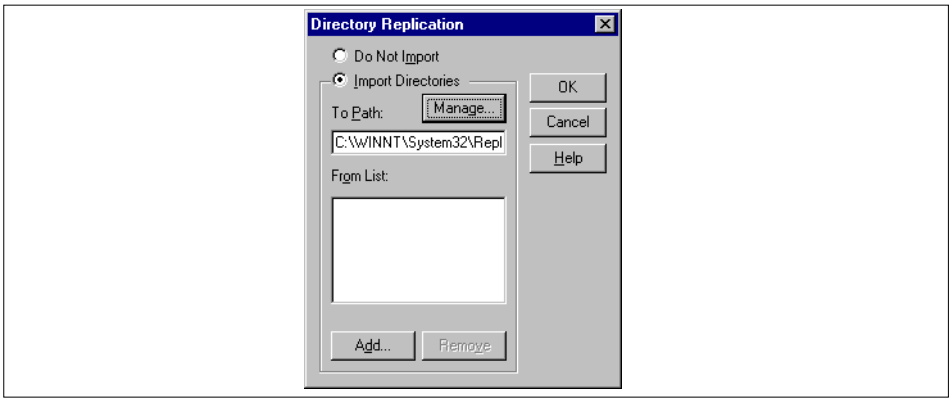


Figure 189. Directory Replication Import Settings

12.Click on **OK**.

13.The directory replicator service is started on the Windows NT workstation.

Since we have already created two files in the test directory on the AS/U server, the directories will be automatically replicated (see Figure 190).

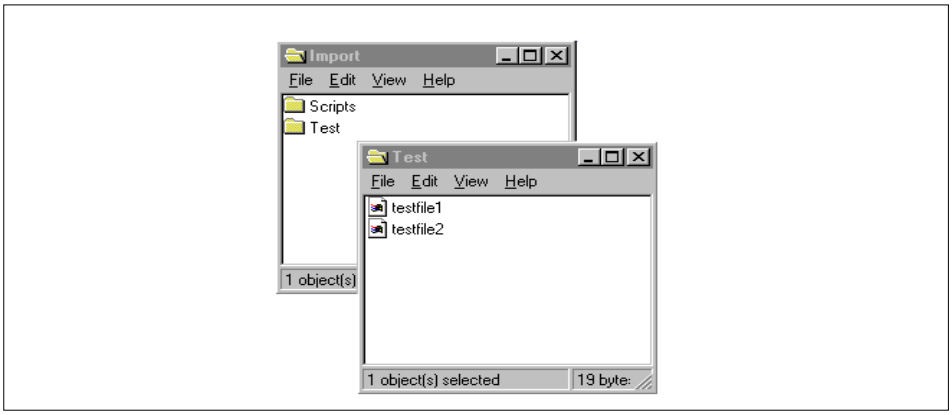


Figure 190. Viewing the Replicated Files

6.8.2 Locking Import Directories

If you want the import system to temporarily stop replications from the server, you can lock the import directory by performing the following steps:

1. Start the **Server** program in the control panel.
2. Select **Replication**.

3. Click on **Manage**.
4. Highlight **Test**.
5. Click on **Add Lock** (see Figure 191).

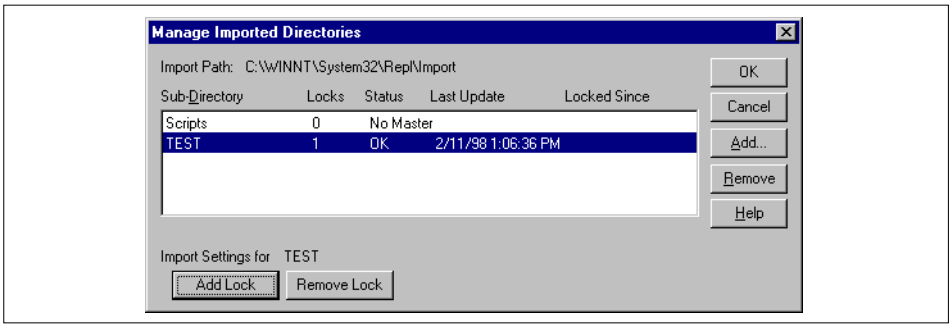


Figure 191. Adding a Lock to an Import Directory

6. Click on **OK**.
7. Click on **OK**.
8. Click on **OK**.

To remove the lock, perform the same steps as above, but in step 5 click on **Remove Lock.**

6.8.3 Directory Replication Registry Settings

There are several registry settings that control the replicator service. These are stored in SYSTEM/CurrentControlSet/Services/Replicator/Parameters. Items of interest are:

Interval Specifies how often, in minutes, an export server checks the replicated directories for changes (default is five minutes).

MaxFilesInDirectory Specifies the maximum number of files in an import directory that can be replicated (default is 2000).

Pulse Specifies how often, in minutes, the export server repeats sending the last update notice (default is three minutes).

To change the maximum number of files that can be replicated, use the `regconfig` command:

```
regconfig SYSTEM/CurrentControlSet/Services/Replicator/Parameters \
```

```
MaxFilesInDirectory REG_DWORD 3000
```

6.9 Trust Relationships

Trust relationships between domains can quickly be established. For a one-way trust relationship to occur, we must perform some configuration in both domains (the trusted and the trusting domain).

6.9.1 Configuring a Trust Relationship

We currently have our own domain, lv3010a_dom in our test environment. To allow users from another domain, lv3010, to log on to machines in our domain using the user accounts stored in their domain, we can perform the following.

6.9.1.1 Configuring the Trusted Domain

The first configuration task takes place in the lv3010 domain. We can perform this from the AS/U server (where the administrator password for the domain lv3010 is test3010) by remotely logging on to the Windows NT server and running the `net` command. To configure a trust relationship we have to specify a password to be used in the relationship. In the following example we use the password, test:

```
net logon administrator test3010 /domain:lv3010
net trust lv3010a_dom /allow test /domain:lv3010
```

Alternatively, we can configure this from the Windows NT server:

1. Log in to the **lv3010** domain.
2. Start the **User Manager** in the lv3010 domain.
3. Select the **Policies** menu.
4. Select the **Trust Relationships** menu item.
5. Click on **Add**, next to the Trusting Domains item.
6. Fill-in the requested information (see Figure 192):
    1. Trusting Domain - **lv3010a_dom**.
    2. Initial Password - **test**.
    3. Confirm Password - **test**.
    4. Click on **OK**.

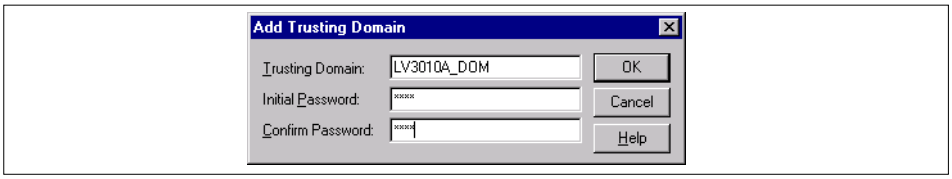


Figure 192. Adding Information for Trusting Domain

One-half of the trust relationship is now established. Figure 193 shows the Trust Relationship window, showing that the lv3010a_dom domain is now known in the lv3010 domain as a trusting domain.

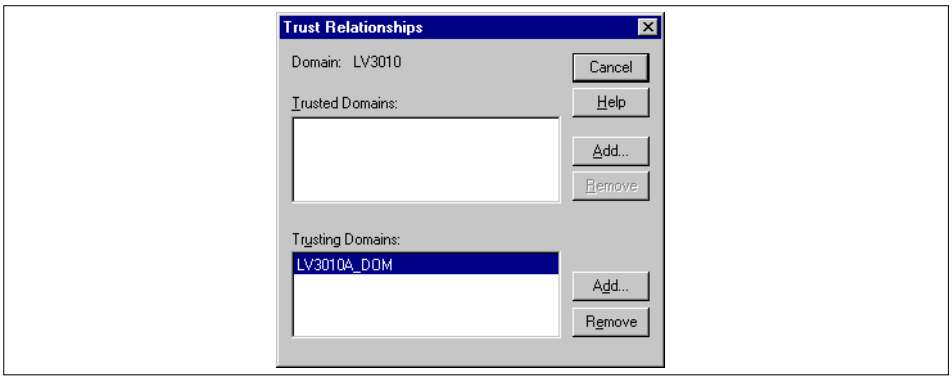


Figure 193. lv3010 Trust Relationships Window

6.9.1.2 Configuring the Trusting Domain

The second part of the configuration takes place in the lv3010a_dom domain. To complete the configuration, either use the `net` command on the AS/U server:

```
# net trust lv3010 /ADD test
```

Or perform the following steps on a Windows NT system:

1. Log in to the **lv3010a_dom** domain.
2. Start **User Manager** (in the lv3010a_dom domain).
3. Select **Policies** menu.
4. Select **Trust Relationships**.
5. Click on **Add** (next to Trusted Domains).
6. Type in the requested information (see Figure 194):
    1. Domain - **lv3010**.

2. Password - **test**.
3. Click on **OK**.

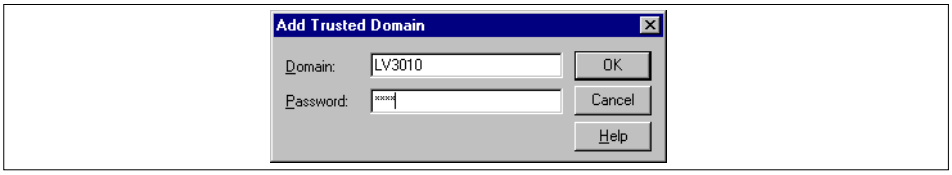


Figure 194. Adding Information for Trusted Domain

If the trust relationship is established, a confirmation box appears (as shown in Figure 195).

Figure 195. Trust Relationship Established Window

We can now see the lv3010 as trusted domain in the Trust Relationships window (see Figure 196).

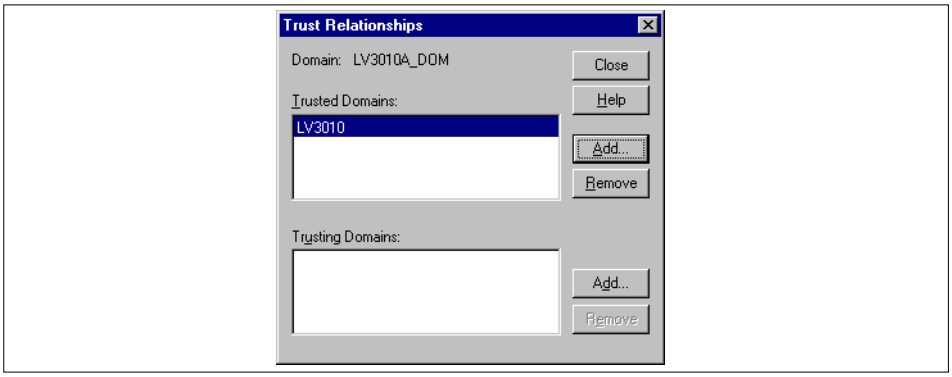


Figure 196. lv3010a_dom Trust Relationships Window

6.9.2 Viewing the Trust Relationships from AS/U

From the AS/U server we can view the trust relationship (in the lv3010a_dom domain) using the net command:

```
# net trust
Advanced Server 4.0 for UNIX.
Domain:    lv3010a_dom
Trusted Domains:
-------------------------------------------------------------------------------
LV3010

Permitted to Trust this Domain:
-------------------------------------------------------------------------------

There are no entries in the list.

The command completed successfully.
```

We can also use the net command to view the lv3010 domain trust relationship from the AS/U server:

```
# net logon administrator test3010/domain:lv3010
# net trust /domain:lv3010
Advanced Server 4.0 for UNIX.
Domain:    lv3010
Trusted Domains:
-------------------------------------------------------------------------------

There are no entries in the list.


Permitted to Trust this Domain:
-------------------------------------------------------------------------------
lv3010a_dom
The command completed successfully.
```

The trust relationship that has been established should allow users from the lv3010 domain to log in with their user ID and password to any machine in the lv3010a_dom domain.

Establishing a two-way trust relationship between the lv3010 and lv3010a_dom domains requires another one-way trust relationship to be set up between the two domains. To complete a two-way relationship, the steps shown above can be repeated in reverse, where the lv3010 domain becomes the trusting domain and the lv3010a_dom domain becomes the trusted domain.

6.9.3 Removing Trust Relationships

To remove trust relationships, remove each configuration (preferably in reverse order, therefore the last addition would be the first item to remove).

The command to remove lv3010, the trusted domain on the AS/U server, is shown below:

```
net trust lv3010 /delete
```

The commands to remove lv3010a_dom, the trusting domain on the AS/U server, are shown below. The logon step is only required if you haven't previously logged in to the lv3010 domain:

```
net logon administrator test3010 /domain:lv3010
net trust lv3010a_dom /disallow /domain:lv3010
```

6.10 Windows NT Network Installation

The AS/U server can be used for installing PCs on the network with either Windows NT Server or Windows NT Workstation. The contents of the Windows NT CDs are copied to the AS/U server into a shared directory. AS/U has a default directory for these files, /var/opt/lanman/shares/msclient. This directory is actually part of the /usr file system. The directory has already been shared as MSCLIENT from AS/U.

6.10.1 Network Installation Setup

To enable network installation, we must copy the contents of the clients directory on the Windows NT Server CD-ROM into the /var/opt/lanman/shares/msclient directory. These are the files that are used to create the installation diskettes. The files can be copied by using the following commands:

```
mount -o ro -v cdrfs /dev/cd0 /mnt
cp -r /mnt/clients/* /var/opt/lanman/shares/msclient
unmount /mnt
```

The second step is to create directories in the /var/opt/lanman/shares/msclient directory for the install images, as shown below:

```
mkdir -p /var/opt/lanman/shares/msclient/winnt/netsetup
mkdir -p /var/opt/lanman/shares/msclient/winnt.srv/netsetup
```

After creating these directories, copy the i386 directory (which requires 90 MB of space in /usr) from the Windows NT Workstation CD-ROM into the winnt/netsetup directory:

```
mount -o ro -v cdrfs /dev/cd0 /mnt
cp -r /mnt/i386/* /var/opt/lanman/shares/msclient/winnt/netsetup
unmount /mnt
```

Then copy the i386 directory (which requires 90 MB of space in /usr) from the Windows NT Server CD-ROM into the winnt.srv/netsetup directory:

```
mount -o ro -v cdrfs /dev/cd0 /mnt
cp -r /mnt/i386/* /var/opt/lanman/shares/msclient/winnt.srv/netsetup
unmount /mnt
```

This completes the setup on the AS/U server. All further work is carried out on a Windows NT workstation.

6.10.2 Creating the Windows NT Network Installation Diskette

Windows NT can be installed over the network from the AS/U server using a single network installation diskette. This bootable diskette contains the network adapter driver for the machine that is to be installed and code to connect to the network. Once connected to the network, the disk initiates an install from the copy of Windows NT that is held on the AS/U server.

AS/U comes with a utility, `ncadmin`, to create this installation diskette. Before you run this utility, prepare a 1.44 MB blank diskette. This has to be a bootable disk and therefore must be created from DOS. To create this disk from DOS, insert the blank disk in your disk drive and run the following command:

```
format a: /s
```

To install the `ncadmin` utility from the lv3010a_asu AS/U server, perform the following steps:

1. Log on to a Windows NT workstation with access to lv3010a_asu.
2. Click on the **lv3010a_asu** system in the Network Neighborhood.
3. Click on the **MSCLIENT** shared directory.
4. Click on the **ncadmin** directory.
5. Copy the **winnt** directory to the local system.
6. Click on the local copy of the **winnt** directory.
7. Run the **Setup** program (this installs the `ncadmin` program in the c:\winnt\system32 directory).

Once the `ncadmin` program has been installed it can be used to create the installation diskette required for network installation. For instance, we have a PC that we want to install with an IBM 16/4 Auto Token-Ring ISA network adapter. To create an installation diskette for this machine, we start the c:\winnt\system32\ncadmin program, as shown in figure Figure 197. We then

select the **Make Network Installation Startup Disk** radio button and then click on **Continue**

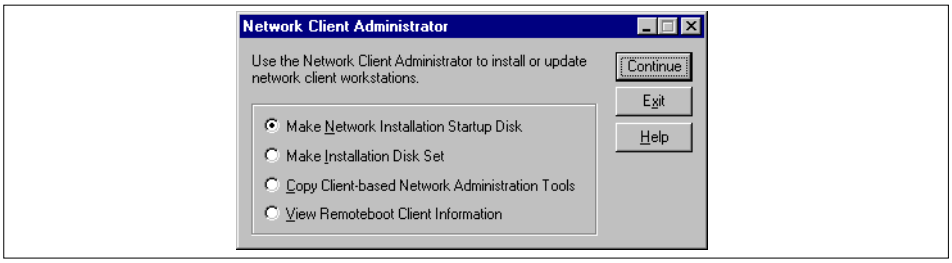


Figure 197. Windows NT ncadmin Program

After clicking Continue, we are presented with a window, as shown in Figure 198, where the path to the network client installation files is entered. Since we have already copied these files to the AS/U server, we select the **Use Existing Path** radio button and enter \\lv3010a_asu\msclient in the **Path** field.

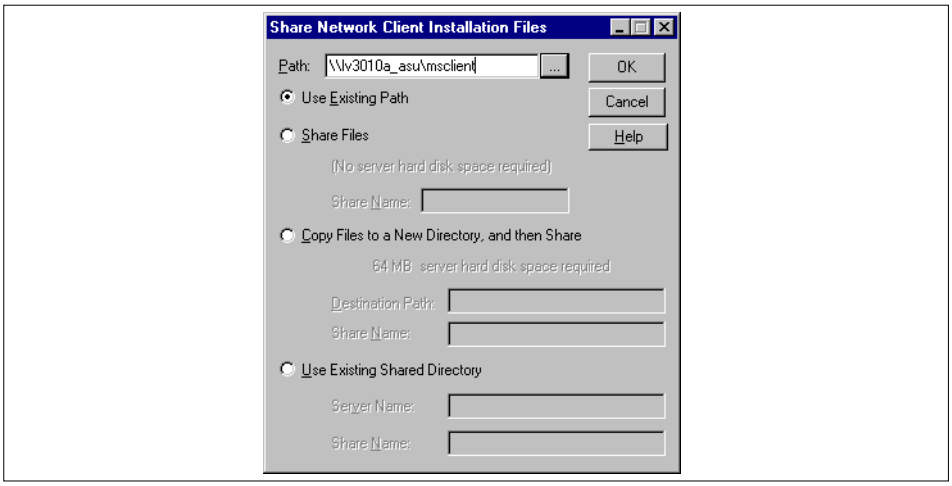


Figure 198. Network Installation Files Location

After completing the information, we click **OK** and are presented with the Target workstation Configuration window, Figure 199. It is here that we select the disk type (in our case a 3.5" diskette) and the platform we will be installing over the network. In this case, we select Windows NT Workstation. At the bottom of the window we must also select the type of network adapter that is in the target machine. In our example we select the IBM Token-Ring (All Types) adapter.

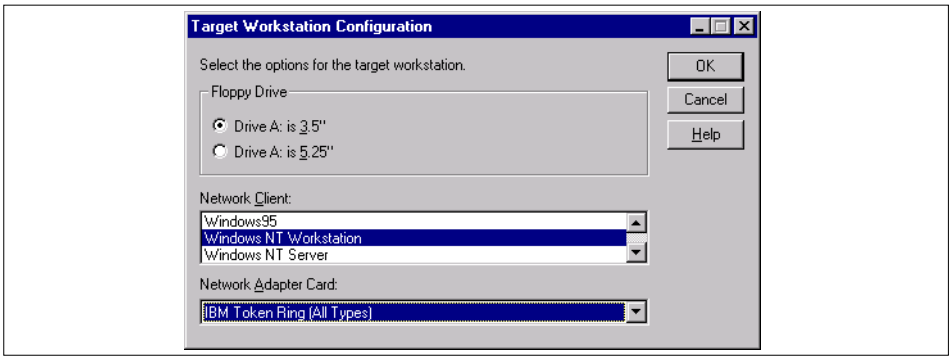


Figure 199. Ncadmin Target Workstation Configuration

After checking the details and clicking **OK**, an information panel is displayed explaining that a license is required to install Windows NT. Click **OK** to continue. This presents us with the Network Startup Disk Configuration window, as shown in Figure 200. This window must be filled-in with TCP/IP details that allow us to connect to the AS/U server. The TCP/IP details here will only be used to get the system started, they will not be automatically entered into the Windows NT installation. Since these details are only used during the start up of the system being installed, we recommend creating a diskette with an unused IP address to use for all network installs (providing that all the machines that will be installed have the same network adapter). You can create one or several disks to use each time a network install is required. The details that we filled-in are shown in Figure 200.

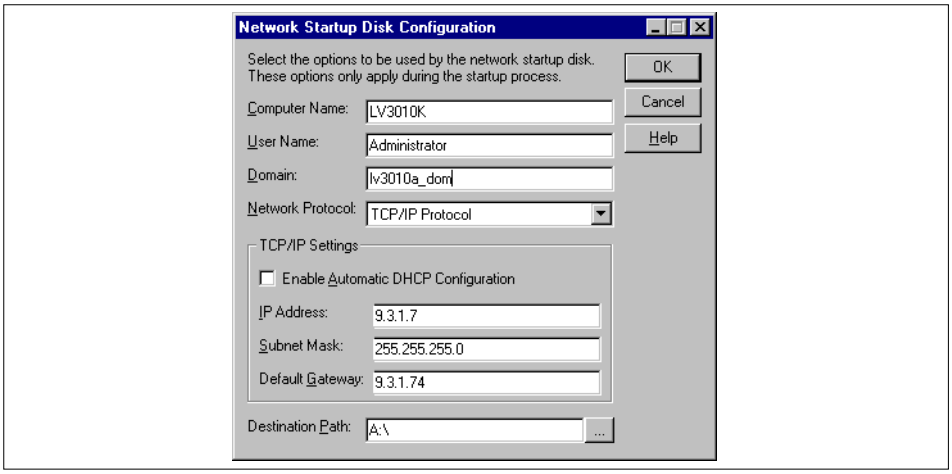


Figure 200. Ncadmin Network Startup Disk Configuration

After entering the details and clicking **OK**, we are given an information message stating that TCP/IP is not available on the selected server. This is not the case, however, and we can still click **OK** to use TCP/IP. After clicking OK, we are presented with a confirmation window, as shown in Figure 201, which asks us to confirm all the details we entered.

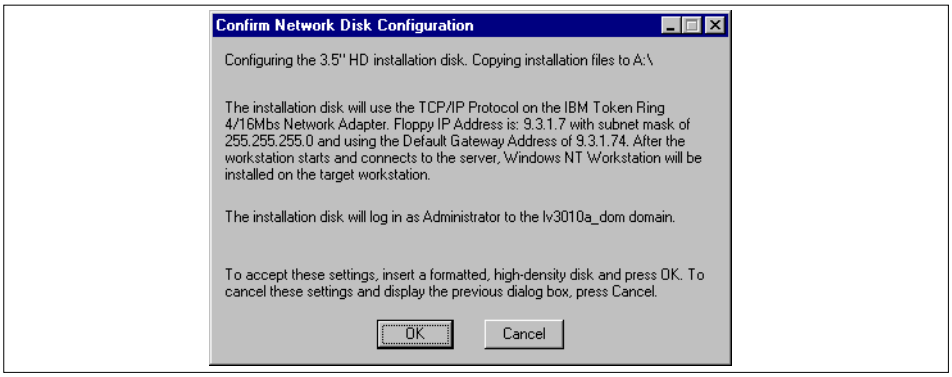


Figure 201. Ncadmin Confirm Network Disk Configuration

After checking the details we can insert the disk that we created. Click **OK** to begin creating the network installation diskette. After the network installation has completed, a window appears, as shown in Figure 202, that says our disk was created successfully.

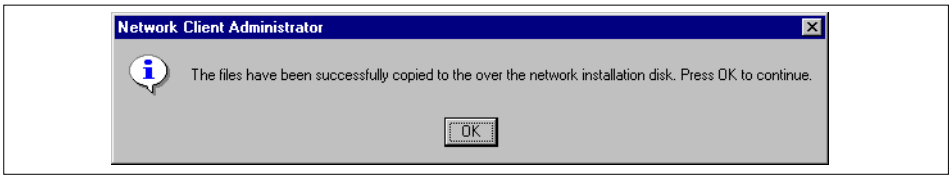


Figure 202. Successful Installation Window

6.10.3 Network Installation

The network Installation disk that was created can now be used to install Windows NT on our target workstation.

6.10.3.1 Initial System Setup

Before we install our target system with Windows NT, we have to create a FAT partition on the system that will be used for the installation. This can be set up from DOS and must be at least 119 MB. This step could be automated and included on the network installation disk. For our test, we created a 500 Megabyte partition on the internal disk of our target system. After the partition is created we can install the system by performing the following steps:

1. Insert the network installation diskette in the disk drive of the target system.
2. Turn on the system.

6.10.3.2 Installing the System

The system will now boot from the diskette. Although the process will install Windows NT, a message will appear stating that the disk is starting Windows 95. Several commands will run, starting the network. A prompt will appear asking for the user name (which defaults to administrator) and the password. We recommend creating an installation user on the AS/U server, specifically for network installations. You will then be asked to create a password list file for the administrator (or user name that was used), select **Yes**. After confirming the password, the install process connects the Z: drive to the \\lv3010a_asu\msclient network directory. After the network drive has been created, the NT installation starts and files are copied from the AS/U server to the target system. Once the files have been copied, the system is restarted to continue the standard Windows NT installation. During the installation we have to enter the TCP/IP configuration, since the installation diskette details are not used.

6.11 WINS Server

WINS is an integral part of AS/U. The service allows AS/U to translate NetBIOS computer names (not DNS host names) into IP addresses.

6.11.1 Starting the WINS Server

To start the WINS server, use the `net` command:

```
# net start wins
Advanced Server 4.0 for UNIX configured for temporary use.
The WINS service is starting.................
The WINS service was started successfully.
```

WINS can also be started from Windows NT using the Server Manager:

1. Log in to Windows NT as administrator in the lv3010a_dom.
2. Start Services Manager.
3. Click on **lv3010a_asu**.
4. Select the **Computer** menu.
5. Select the **Services** menu item.

6. Click on **Windows Internet Name Service** (see Figure 203).
7. Click on **Start**.

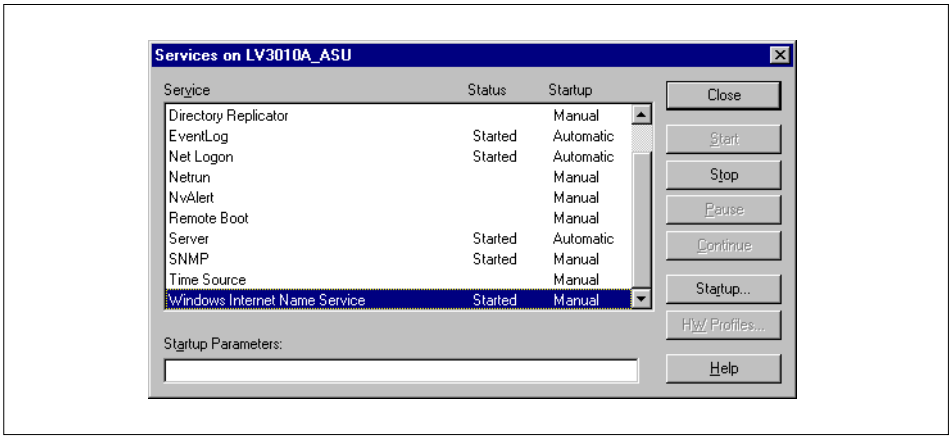


Figure 203. Starting the WINS Service

6.11.2 Configuring WINS to Start Automatically

The WINS service can be started automatically when AS/U is started (the default is a manual start). To configure AS/U to start WINS automatically, add the WINS service to the lanman.ini file by using the following SMIT command:

```
smit advanced_server_lanman
```

Add **wins** to the Services automatically started field (shown in Figure 204 on page 248).

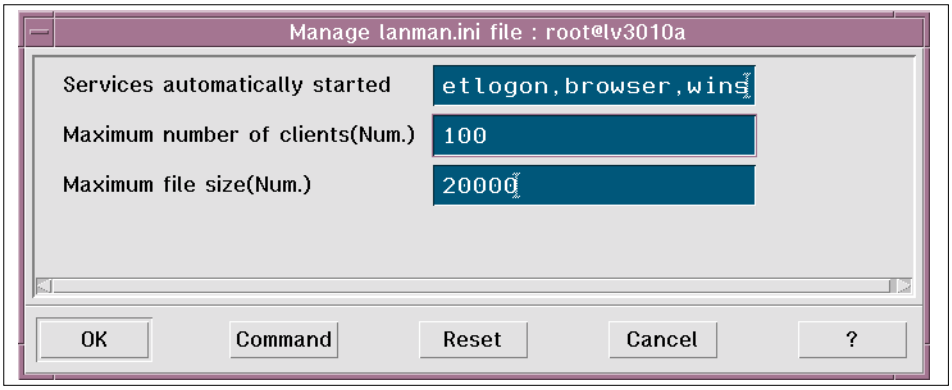


Figure 204. SMIT - Manage lanman.ini File

When AS/U restarts, WINS automatically starts along with the other configured services.

6.11.3 Administering WINS

WINS is administered from Windows NT using the `winsadmn` utility that was installed with the other AS/U tools.

To configure the WINS AS/U server, perform the following steps:

1. Start the winsadmn program (`c:\winnt\system32\winsadmn`).
2. Select the **Server** menu.
3. Select the **Add WINS Server** menu item.
4. In the dialog box, enter the name of the WINS system - **lv3010a_asu**.
5. Click on **OK**.

If a dialog box appears stating that the WINS server cannot be validated, enter the IP address of the AS/U server, **lv3010a_asu** (see Figure 205).

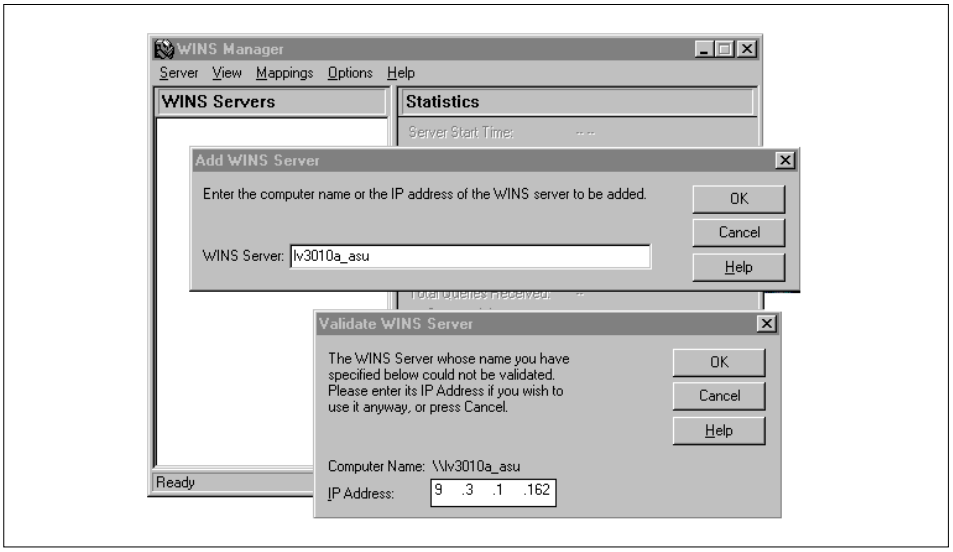


Figure 205. Validation of WINS Server

Once the details of the WINS AS/U server have been entered, the `winsadmn` utility shows the details of the WINS system in its main window (see Figure 206).

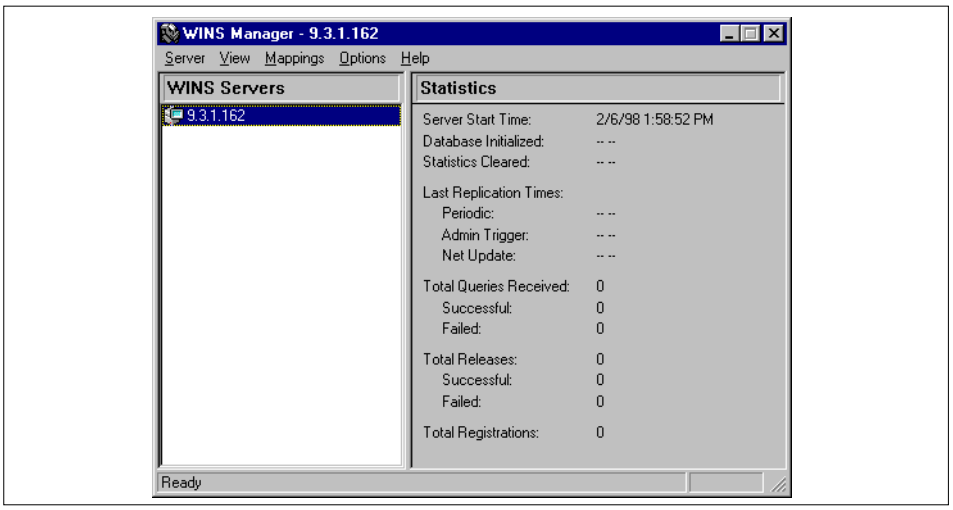


Figure 206. winsadmn Main Window

6.11.4 Configuring a WINS Client

We can set up a Windows NT system to use the AS/U server as the WINS server. Configuring a client to use a WINS server means that all requests to convert a system name to an IP address are made to the WINS server. If the request is unsuccessful a broadcast is made to obtain the IP address. To configure this, perform the following steps (in our example we use a Windows NT workstation called lv3010k, with IP address 9.3.1.162):

1. Open the **Network** program in the control panel.
2. Select **Protocols**.
3. Click on **TCP/IP Protocol**.
4. Fill-in the IP address of the WINS Server (see Figure 207).
5. Reboot the Windows NT system.

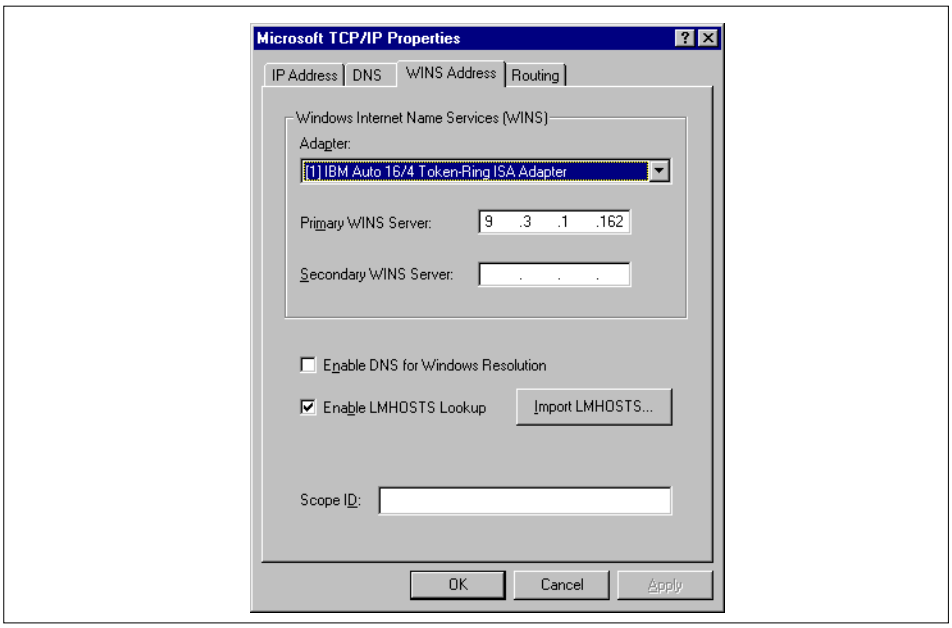


Figure 207. Configuring WINS Client

6.11.5 Displaying the WINS Database

We can view the WINS database on the AS/U server with the `winsadm` program. To do so, perform the following steps:

1. Open the **`winsadm`** program.
2. Select the **Mappings** menu.
3. Select the **Show Database** item.

This presents a window (see Figure 208) showing all the computer name to IP address mappings that are stored in the WINS database.

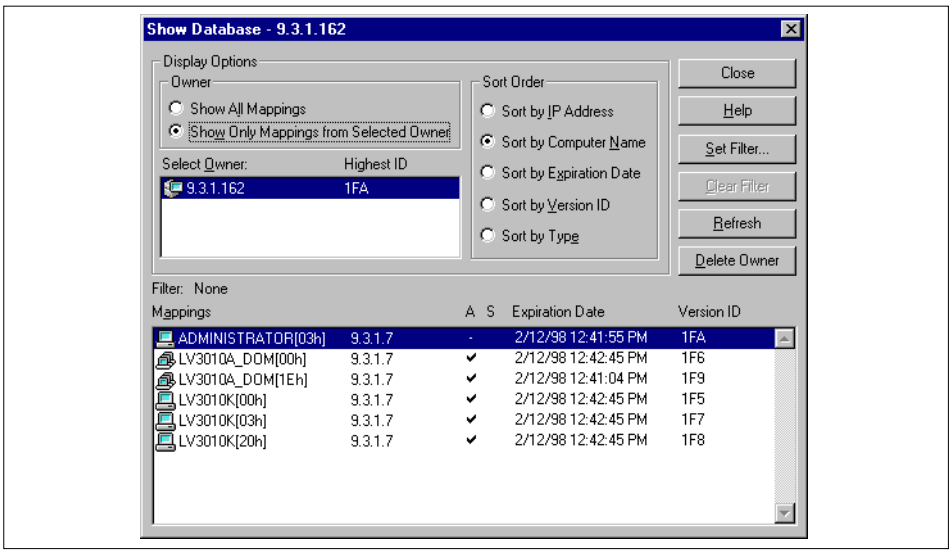


Figure 208. Show WINS Database

6.11.6 WINS Static Mappings

Static mappings can be added to the WINS database for systems that are not automatically picked up through client registration or replication. If we have a system called lv3010b with IP address 9.3.1.163, we can add this to the database by using the `winsadmn` utility:

1. Start the **`winsadmn`** utility.
2. Click on the WINS server (in our example, 9.3.1.162).
3. Select the **Mappings** menu.
4. Select the **Static Mappings** menu item.
5. Click **Add Mappings**.
6. This presents a window, as shown in Figure 209.

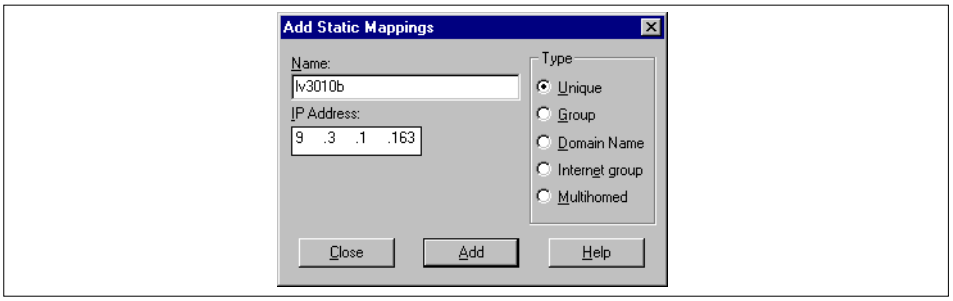


Figure 209. WINS Add Static Mapping

Fill-in the name of the system, lv3010b, and the IP address, 9.3.1.163. After completing the information, click **Add**. In the main Add Static Mapping window, you can see the mapping for the system, lv3010b (see Figure 210).

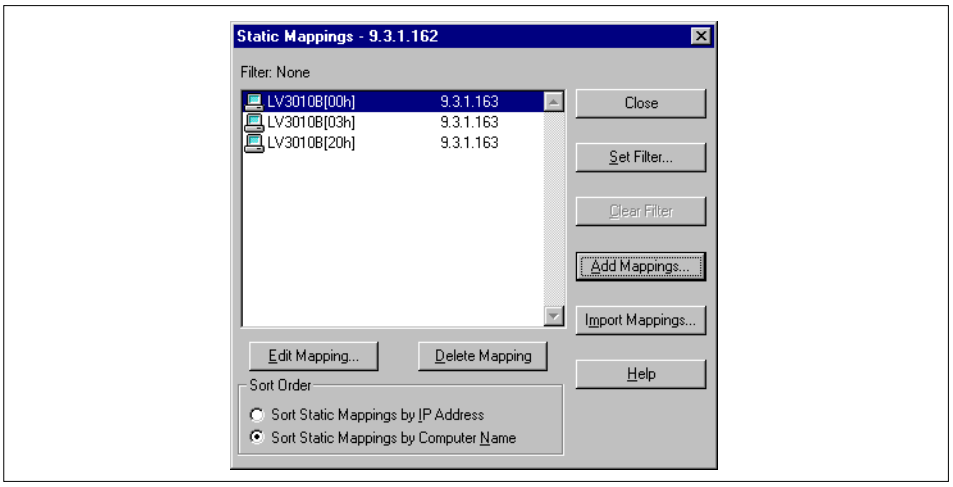


Figure 210. WINS Static Mappings

When you display the WINS database the lv3010b system is now listed. Whenever clients who use the WINS database look for the lv3010b system, they will be returned the IP address from the WINS AS/U server.

Names that are not in the WINS database are resolved using broadcasts. If our client system wants to find a system not in the WINS database, it broadcasts a message to all machines stating that it is looking for the system. It is wise, therefore, to maximize the number of systems registered in the WINS database to cut down on network traffic. The ideal large network

consists of several WINS servers, perhaps one for each local network. Each WINS server will replicate information from other WINS servers.

6.11.7 WINS Replication

The AS/U WINS server can be set up to replicate to and from other WINS servers. Replication is configured by adding push and pull partners:

Pull partner A pull partner is a WINS server that pulls WINS database entries from its push partners.

Push partner A push partner is a WINS server that sends messages to pull partners to inform them that the WINS database has changed. Pull partners respond to the messages by sending a replication request. The push partner then sends a copy of the new WINS database entries.

In our network, we have another WINS server (lv3010f in the lv3010 domain) from which we want to obtain WINS database updates. We have to configure both WINS servers, the AS/U server, lv3010a_asu and lv3010f.

Since we want the lv3010f WINS server to be a push partner to lv3010a_asu, we first configure our AS/U server to include lv3010f as a push partner:

1. Log on as **administrator** on a Windows NT system in the lv3010a_dom domain.
2. Run the **Winsadmn** program.
3. Select the **AS/U Server** on the main window (9.3.1.162 in our example).
4. Select the **Server** menu.
5. Select the **Replication Partners** menu item.
6. Click **Add**.
7. Enter the name of the WINS server to add - **lv3010f** (9.3.1.124).

After the server has been added we can configure it as a push and/or pull partner. We want to add it as a push partner, so we perform the following steps:

1. Click on the **Replication Server** - 9.3.1.124.
2. Select the **Push Partner** radio button.

The WINS server lv3010f is now a push replication partner (as shown in Figure 211).

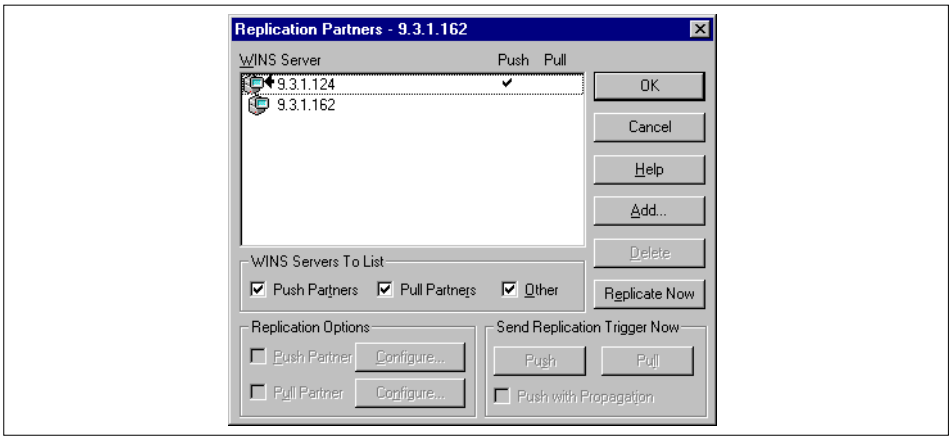


Figure 211. WINS Window for Push Replication Partner

If we click on the **Configure...** button (for the push parameter), we can set the update count (see Figure 212). The update count is the number of changes that are required to be made to the WINS database before a replication message is sent to the replication partner.

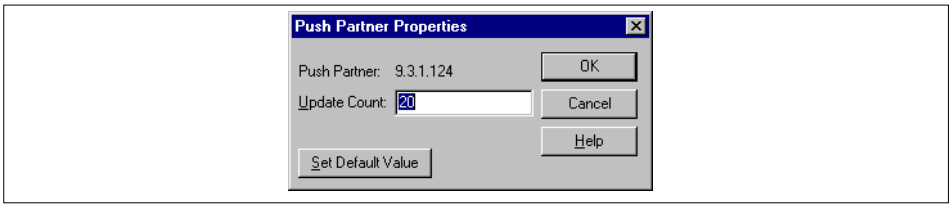


Figure 212. WINS Push Replication Properties

Now that the push replication settings have been completed we can configure the pull replication settings:

1. Log on as **administrator** on a Windows NT system in the lv3010 domain.
2. Run the **winsadm** program.
3. Select the lv3010f server on the main window (**9.3.1.124** in our example).
4. Select the **Server** menu.
5. Select the **Replication Partners** menu item.
6. Click **Add**.
7. Enter the name of the WINS server to add - **lv3010a_asu** (9.3.1.162).

After the server has been added we can configure it as a push and/or pull partner. We would like to add it as a pull partner so we perform the following steps:

1. Click on the Replication server - **9.3.1.162**.
2. Select the **Pull Partner** radio button.

The WINS server lv3010a_asu is now a pull replication partner (as shown in Figure 213).

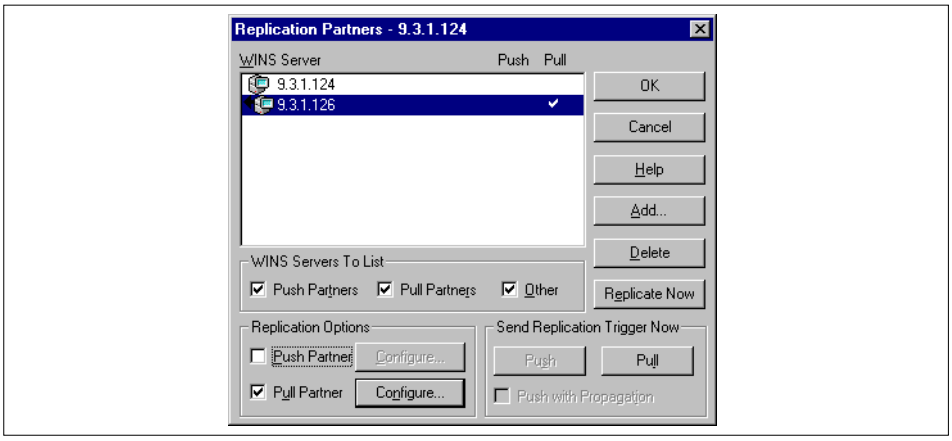


Figure 213. WINS Window for Pull Replication Partner

If we click on the **Configure...** button (for the pull parameter), we can set the start time for the replication and the replication interval (see Figure 214). The interval setting depends on how busy your network is and how regularly changes are made. To reduce network traffic, we recommend setting the replication interval quite high (unless many changes are being made to your network).

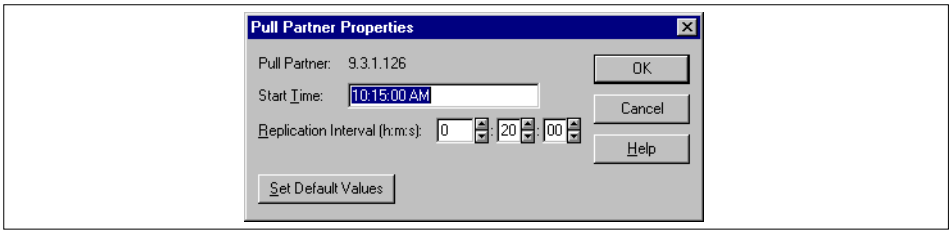


Figure 214. WINS Pull Replication Properties

Now that replication has been configured, updates will occur automatically.

6.12 Changing the Domain Name

As your network grows you may find that the original domain name is not suitable. AS/U can change its domain name using the `setdomainname` command. For the new domain name to be active throughout the domain, all members have to change their domain name to the new name. Be aware that any changes to the domain name require all trust relationships to be re-created using the new domain name.

6.12.1 Changing the Domain Name on AS/U

In our setup, AS/U is the primary domain controller. We must first change its domain name using the `setdomain` command. The AS/U server is stopped when this command executes. If the `-s` option is used, AS/U does not restart after changing the domain name and will have to be started manually. We found that if we let the `setdomainname` command restart AS/U, an error message was displayed stating that AS/U couldn't be restarted (although it appeared to be up and running with no problems). The following lines change the AS/U domain name of the lv3010a_asu server from lv3010a_dom to lvdom1, and restart the AS/U server:

```
setdomainname -n lvdom1 -s
/etc/rc.asu start
```

6.12.2 Changing the Domain Name on the PDC

After we change the PDC domain name we must change the BDC domain name to be the same. If the BDC is a Windows NT Server we can change the domain name using the following process:

1. Log on as **administrator** in the lv3010a_dom domain.
2. Open the **Network** item in the control panel.
3. On the identification panel select **Change**.
4. Enter the new domain name - **lvdom1** (seeFigure 215).
5. Click **OK**.
6. The system is welcomed into the lvdom1 domain.
7. Close the **Network** program.
8. Restart the system.

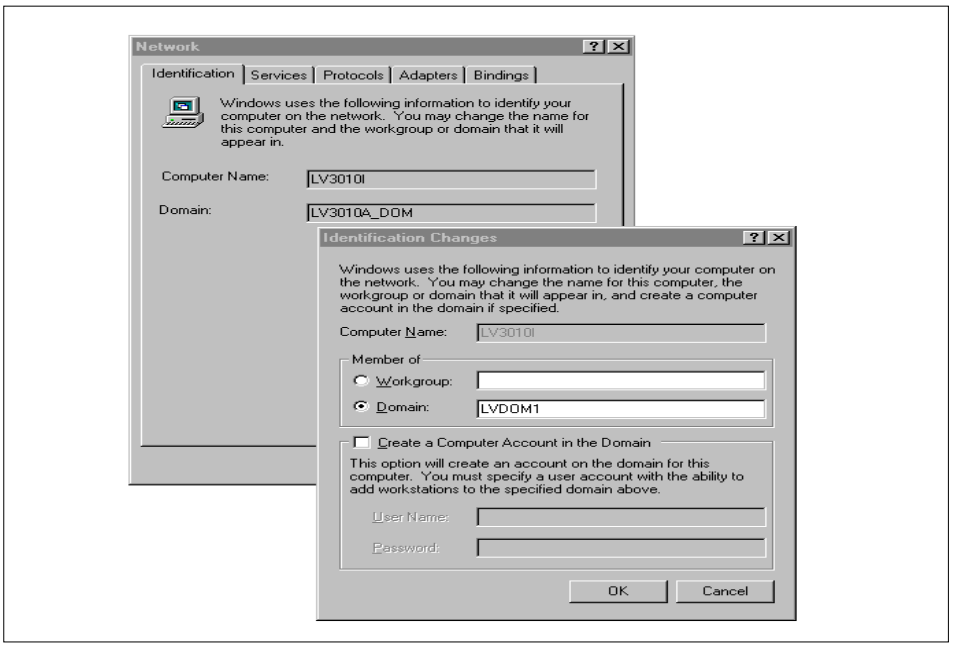


Figure 215. Changing Backup Domain Controller Domain

If the BDC is another AS/U server, we can use the `setdomainname` command and restart the AS/U server:

```
setdomainname -n lvdom1 -s
/etc/rc.asu start
```

Once the PDC is rebooted with the new domain name it will still be the BDC to our AS/U PDC (SAM replications will continue).

6.12.3 Changing the Domain Name on Other Domain Members

After the PDC and BDC have had the domain name changed, we can change the other members of the domain. Member servers in the domain can use the process described in 6.12.2, “Changing the Domain Name on the PDC” on page 257. In our network we have a Windows NT workstation that is part of the original lv3010a_dom domain. We can change this to the new domain using the following process:

1. Logon as **administrator** on the local system.
2. Open the **Network** item in the control panel.
3. On the identification panel, select **Change**.

4. Enter the new domain name - **lvdom1** (see Figure 216). Do not select Create a Computer Account in this Domain, since one already exists.
5. Click **OK**.
6. A warning message appears asking if you really want to make the change, since users may not be able to log on after the change. Select **Yes**.
7. The system is welcomed into the lvdom1 domain.
8. Close the **Network** program.
9. Restart the system.

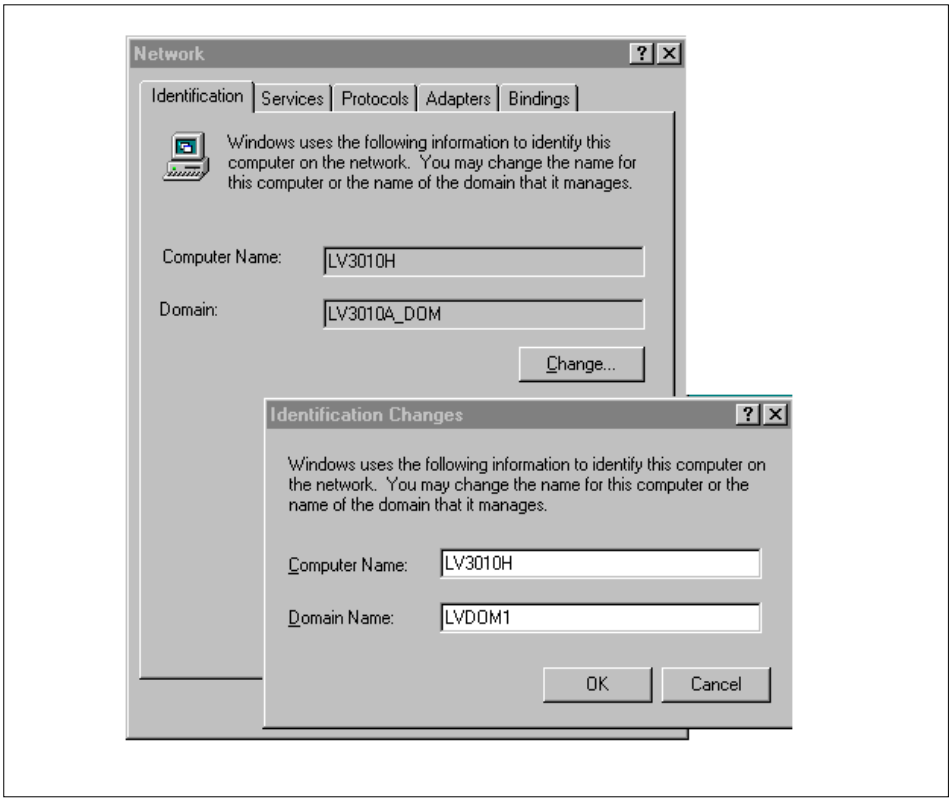


Figure 216. Changing Workstation Domain

Once the system has been rebooted, it will be part of the new lvdom1 domain. Existing users in the lv3010a_dom will be able to log on to the workstation.

6.13 Changing the Domain Role of AS/U

There may be situations where you want the BDC in your network to be promoted to the PDC, as described in the following list:

- After configuration of AS/U as a PDC and another system as a BDC, you decide that you want to switch the role of your AS/U server to a BDC. This is done with both domain controllers online
- The AS/U server acting as a PDC has failed and is not available, and you need to promote the BDC to become the PDC until the AS/U server is back online.

Alternatively, your AS/U server may configured as the BDC and you would like to promote it to the PDC.

6.13.1 Promoting a Windows NT BDC

On our network we have configured the AS/U server, lv3010a_asu, as the PDC in the lv3010a_dom domain. The BDC is a Windows NT server, lv3010h.

6.13.1.1 Promoting Windows NT to PDC when the PDC is Online

To promote the Windows NT server to become the PDC while the AS/U server is running, we perform the following steps. During the process, the AS/U server will automatically be demoted to the BDC:

1. Log on to the Windows NT server, lv3010h, as **administrator** in the lv3010a_dom domain.
2. Run the server manager program - `srvmgr`.
3. Highlight the lv3010h Windows NT 4.0 Backup entry in the server manager window.
4. Select the **Computer** menu.
5. Select the **Promote to Primary Domain Controller** menu item.
6. A window appears, explaining that the process may take a few minutes and any users will be disconnected (see Figure 217).

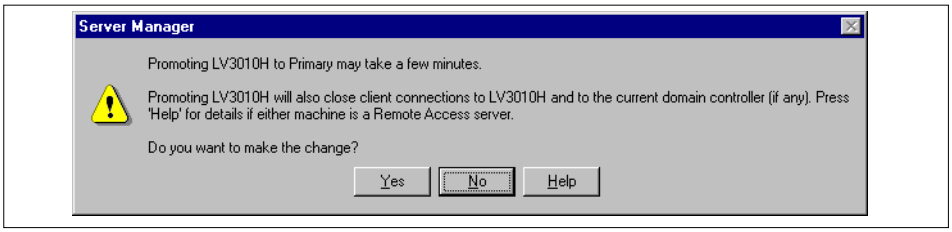


Figure 217. Promoting Windows NT BDC to PDC Information Message

7. Click **Yes**.
8. The process of switching the roles of the domain controllers begins. The first step is to synchronize the SAM database between the current PDC and BDC (see Figure 218).

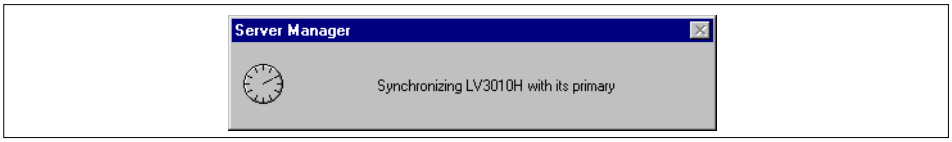


Figure 218. Synchronizing Data from PDC

9. Messages will appear explaining the tasks which are being completed.

Once the process has completed, the domain controller's roles are switched and services are restarted on both systems. In the Server Manager window, we can now see that the Windows NT server is now the PDC (see Figure 219).

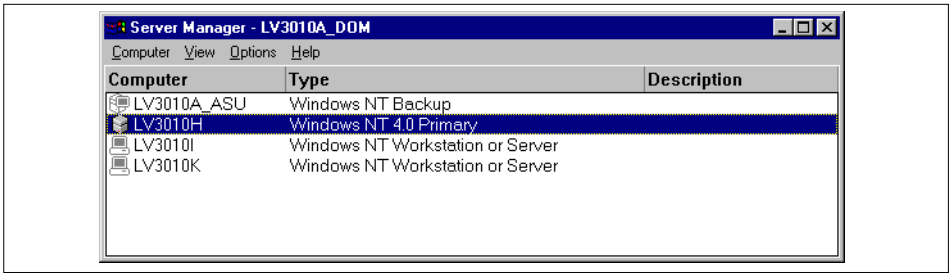


Figure 219. Server Manager Window Showing New Roles for Domain Controllers

6.13.1.2 Promoting Windows NT to PDC when the PDC is Offline

To promote the Windows NT server to become the PDC while the AS/U server is not running, we can use the same procedure as described in

6.13.1.1, “Promoting Windows NT to PDC when the PDC is Online” on page 260. Since the AS/U server is not available, it will not automatically be demoted to the BDC during the process.

When the AS/U system is available we can demote it to a BDC by running the `joindomain` command on the AS/U server, before starting AS/U. If the AS/U server is running, `joindomain` will stop it. The following screen shows the steps to go through using the `joindomain` command:

```
# joindomain
The Advanced Server for UNIX Systems configuration utility (joindomain)
allows you to specify the server name, the domain name, and the server's role
within that domain. Each time you run this utility, the server
will be stopped and the user accounts database and associated files will be
re-initialized. All data currently in those files will be replaced.

Do you want to continue [y/n]? y

The current name of this server is (lv3010a_asu).
Would you like to change this name now [y/n]? n

This server is configured as a 'primary' domain controller.
Would you like to change the role of this server to 'backup' [y/n]? y

This server will become a 'backup' domain controller.
Enter the name of the primary domain controller: lv3010h

Enter the name of an administrator account on 'lv3010h'
or press Enter to select 'administrator':

Enter the password for administrator:
Re-enter password:

Contacting the server 'lv3010h' ... Success

Confirm choices:         servername   : lv3010a_asu
                         role         : backup
                         domain       : LV3010A_DOM
                         primary      : lv3010h
Is this correct [y/n]? y

Creating Advanced Server for UNIX Systems accounts database.

Do you want to start the server now [y/n]? n
# /etc/rc.asu start
```

We found that after running the steps above, we need to synchronize from the Windows NT PDC and then stop and restart the AS/U server to complete the operation. To do so, perform the following steps:

1. Start the server manager, `svrmgr`, on the Windows NT BDC.

2. Highlight **lv3010h** (the Windows NT PDC).
3. Select the **Computer** menu.
4. Select the **Synchronize Entire Domain** menu item.
5. Start and stop the AS/U server from the AS/U system:

```
/etc/rc.asu stop
/etc/rc.asu start
```

6.13.2 Configuring AS/U as a Backup Domain Controller

During the initial installation of AS/U, AS/U can be set up and configured as a backup domain controller. To do so, follow the procedures described in Section 6.2, “Advanced Server for UNIX Installation” on page 186. However, in Section 6.2.6, “Initial Setup” on page 188, select **Backup** as the role of the server. You are then be asked for the name of the PDC and the administrator account and password. After completing these steps, AS/U is configured and running as a BDC.

6.13.3 Promoting an AS/U BDC

On our network we have configured the AS/U server, lv3010a_asu, as the BDC in the lv3010a_dom domain. The PDC is a Windows NT server, lv3010h.

6.13.3.1 Promoting AS/U to PDC when the PDC is Online

To promote the AS/U server, lv3010a_asu, to become the PDC while the Windows NT server is running, we can use the same procedure as described in 6.13.1.1, “Promoting Windows NT to PDC when the PDC is Online” on page 260. However, you must highlight the lv3010a_asu backup domain controller system instead of the Windows NT system (the Windows NT server will automatically be demoted during the process to the BDC). We tried to promote the AS/U server using the AS/U command, `joindomain`, but it failed and left the server in an unstable state.

6.13.3.2 Promoting AS/U to PDC when the PDC is Offline

To promote the AS/U server, lv3010a_asu, to become the PDC while the Windows NT server is offline, we can use the same procedure as described in 6.13.1.1, “Promoting Windows NT to PDC when the PDC is Online” on page 260. Since the PDC is not available we can use another Windows NT system on the network and log on to the AS/U server, highlighting the lv3010a_asu backup domain controller system instead of the Windows NT system. The Windows NT server will not automatically be demoted to the BDC during the process.

When the Windows NT system becomes available again, it can be changed to a BDC by performing the following steps:

1. Start the Windows NT system (the former PDC). When the Windows NT system starts, it detects that there is another PDC on the network and the NETLOGON service will fail. An error will appear in the event log (see Figure 220).

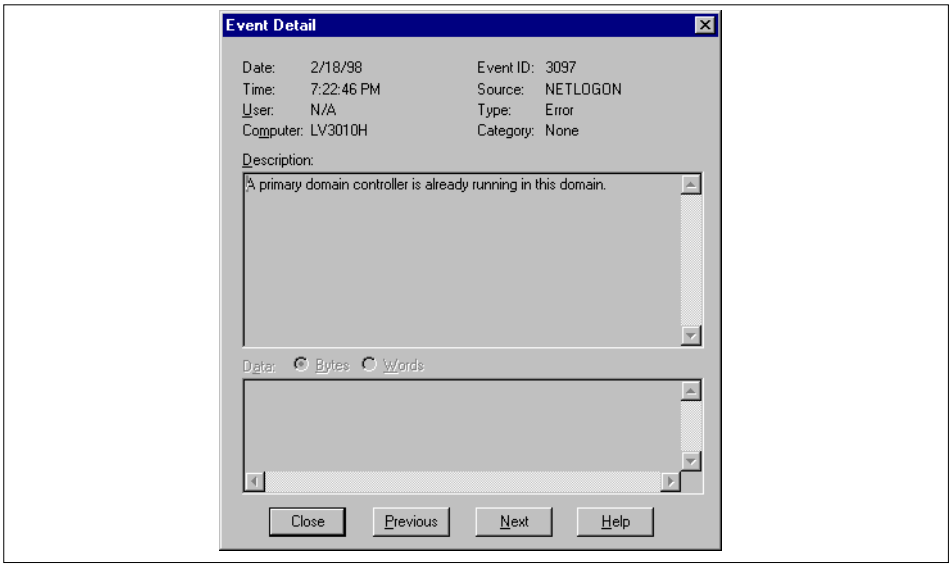


Figure 220. Event Viewer Showing NETLOGON Failure

2. Restart Windows NT.
3. Run the **Server Manager** program, `svrmgr`.
4. If the Windows NT system and the AS/U server are both showing as PDCs, then highlight the Windows NT system (lv3010h in our example). If the Windows NT system is not showing as a PDC, then restart Windows NT and repeat this step.
5. Select the **Computer** menu.
6. Select the **Demote to Backup Domain Controller** menu item.
7. Restart Windows NT.

Windows NT will reboot, start the NETLOGON service and synchronize the SAM database from the AS/U server.

6.14 Recommendations

We recommend that the Windows NT workstation has an NTFS file system for the Windows NT partition. Using FAT will not allow the security benefits of NTFS (file access granularity and so forth). Without NTFS there will only be one recycle bin, and all users will be able to see deleted files of other users and delete the files. If the file system is NTFS, each individual user will have their own recycle bin and not be able to see the deleted files of other users. A FAT file system can be converted to an NTFS file system with the Windows NT `convert` utility. The conversion can be performed with the following command:

```
convert c: /fs:ntfs
```

The conversion will not take place until the Windows NT system has been rebooted. During the reboot Windows NT will convert the file system to NTFS.

6.15 Limitations

AS/U has a few limitations. This section discusses them, some of which may be mentioned elsewhere in this chapter.

6.15.1 WINS Restrictions

If you are administering WINS from a Windows NT workstation with `winsadmn`, you have to use the TCP/IP address of the WINS server and not the NetBIOS name.

6.15.2 Domain Relationship

AS/U can act as a primary or backup domain controller but it cannot be configured as a stand-alone server.

6.15.3 Directory Replication

Export servers can replicate as many subdirectories as required, but each exported subdirectory is limited to 32 subdirectory levels in its tree.

6.15.4 Domain or Server Name

You cannot connect to the domain or server if you use one or more accented characters in the domain or server name.

6.16 Troubleshooting

This section describes problems we came across while testing AS/U and explains how we resolved them. This section also provides some hints about to what to do to detect and work with problems that occur while using AS/U.

6.16.1 Processes

The AS/U installation inserts two lines into the inittab to first start NetBIOS and then AS/U automatically, when the machine boots:

```
rcnetbix:2:wait:/etc/rc.netbix >/dev/console 2>&1 # start NetBIOS for UNIX
rcasu:2:wait:/etc/rc.asu start 2>&1 >/dev/console # Advanced Server for UNIX
```

After NetBIOS starts, the following processes are running:

```
 UID   PID  PPID   C CMD
root 20078     1   0 netbiosd started 0
root 20598     1   0 /usr/bin/NBAudit -start
```

After AS/U starts the following processes are running (there may be more, depending on which services you have told AS/U to start automatically):

```
 UID   PID  PPID   C CMD
root 18724 20368   2 lmx.srv -s 1
root 21142 20368   0 lmx.srv -s 2
root 19752 20368   1 lmx.lpd
root 20368     1   0 lmx.ctrl
root 21304     1   0 lmx.dmn
root 21568     1   0 lmx.alerter
root 21832     1   0 lmx.browser
root 22906     1   0 /usr/net/servers/lanman/snmp/lmxsnmpd -p 4006
```

There may only be one lmx.srv process running. If you have problems and find that the processes listed above are not running, try stopping and restarting AS/U to see if the processes will restart.

6.16.1.1 Viewing Server Processes for Clients

You can find out which clients are connected to which lmx.srv processes by using the `lmstat` command. The `lmstat` command reports which clients are attached to which process ID:

```
# lmstat -c
Shared memory initialization time: Mon Feb 23 17:53:58 1998
Lmx.ctrl's current time:           Wed Feb 25 16:36:06 1998
Server statistics last cleared:    Mon Feb 23 17:53:58 1998
Shared memory size:                396028 bytes

Clients:
     LV3010K (nwnum=0, vcnum=255) on 15882
     LV3010H (nwnum=0, vcnum=255) on 17661

# ps -ef |grep 15882
    root 15882 18948   0   Feb 23      - 16:34 lmx.srv -s 2
#
```

6.16.2 Repairing Database Corruption

AS/U provides two tools to repair corruption:

regcheck, for repairing registry corruption

samcheck, for repairing SAM database corruption

6.16.2.1 regcheck

The regcheck command can be used to view the entire registry in detail, check for corruption and repair corruption. To check for corruption run:

```
regcheck -C
```

To repair corruption:

```
regcheck -R
```

6.16.2.2 samcheck

The samcheck command can be used to view the SAM database, check for corruption and repair corruption. To check for corruption run:

```
samcheck -s
```

To repair corruption:

```
samcheck -r
```

6.16.3 Event Viewing

Like Windows NT, AS/U has an event log. This can be viewed from Windows NT using the Event Viewer or from AS/U with the elfread command.

There are three different types of logs you can view:

- System

- Security
- Application

To view the system log:

```
# elfread  system
--------------------------------------------------------------------------------
DATE      TIME        SOURCE          CATEGORY            EVENT  USER
--------------------------------------------------------------------------------
02/23/98  08:29:54PM  NETLOGON        None                5711   N/A
02/23/98  07:54:03PM  BROWSER         None                8021   N/A
02/23/98  07:41:58PM  BROWSER         None                8021   N/A
02/23/98  07:29:53PM  BROWSER         None                8021   N/A
02/23/98  07:17:50PM  BROWSER         None                8021   N/A
02/23/98  07:05:48PM  BROWSER         None                8021   N/A
02/23/98  06:53:46PM  BROWSER         None                8021   N/A
02/23/98  06:41:44PM  BROWSER         None                8021   N/A
02/23/98  06:29:42PM  BROWSER         None                8021   N/A
02/23/98  06:17:41PM  BROWSER         None                8021   N/A
02/23/98  06:05:39PM  BROWSER         None                8021   N/A
02/23/98  05:54:07PM  Eventlog        None                6005   N/A
02/23/98  05:42:56PM  SERVER          None                6060   N/A
02/23/98  05:42:55PM  BROWSER         None                8033   N/A
```

To view the system events in detail:

```
# elfread -d system
--------------------------------------------------------------------------------
        DATE:     02/23/98            EVENT ID: 5711
        TIME:     08:29:54PM          SOURCE:   NETLOGON
        USER:     N/A                 TYPE:     Information
        COMPUTER: LV3010A_ASU         CATEGORY: None

DESCRIPTION: The partial synchronization request from the server LV3010H
completed successfully. 3 changes(s) has(have) been returned to the caller.
DATA:
```

You can clear the system log with:

```
elfread -c system
```

6.16.4 AFS

If you have AFS installed on the system on which you install AS/U, the setup of AS/U may fail. We found that NetBIOS refused to start and we had to stop AFS and remove the product from our system. After removal of AFS, AS/U was able to work.

6.16.5 Printing

We found that if we tried to delete a print queue from AS/U while a never-ending print job was in progress (meaning it would never complete), this caused AS/U to become unstable. The only way to solve the problem was to reboot the AIX system. To prevent this, delete the print job first. For example, if the print job is number 1005, then delete the printer:

```
net print 1005 /delete
```

6.16.6 Network Installation

When we created our network installation diskette using the `ncadmin` utility, we found that the IBM Token-Ring driver would not work with our network card (an IBM Auto Token-Ring 16/4 Adapter), and we had to download a new version from the IBM PC support Web pages. The URL of the driver diskette including the DOS token-ring driver is:

```
http://www3.pc.ibm.com/techinfo/37be.html
```

This Web page contains an executable file that is used to create the driver diskette for our adapter. Once the diskette was created, we copied the ibmtok.DOS file to our network install diskette over the same file in the net directory. After copying this file we were able to boot from the diskette and start the install from the AS/U server.

6.16.7 Windows NT Miscellaneous

Occasionally, Windows NT can get confused about the network resources that are available on the AS/U server. We found that rebooting the Windows NT workstation would clear up the confusion. For example, after a printer queue was deleted on the AS/U server, Windows NT occasionally presented the printer as available on the server. A reboot cleared the entry.

6.17 Miscellaneous

This section covers additional points that are not covered elsewhere in this chapter.

6.17.1 Mapping Network Drives

Directories that have been shared from AS/U can easily be mapped into drive volumes under Windows NT so they viewed as a drive letter, such as `f:`. If our AS/U server is lv3010a_asu and we have a shared directory called documents, we can use the following procedure to map a drive letter to documents from Windows NT:

1. Click on the AS/U server, **lv3010a_asu**, from within the Network Neighborhood.
2. A list of resources, including the shared directories, appears.
3. Right-click on the shared directory, **DOCUMENTS**, that will be mapped (see Figure 221).

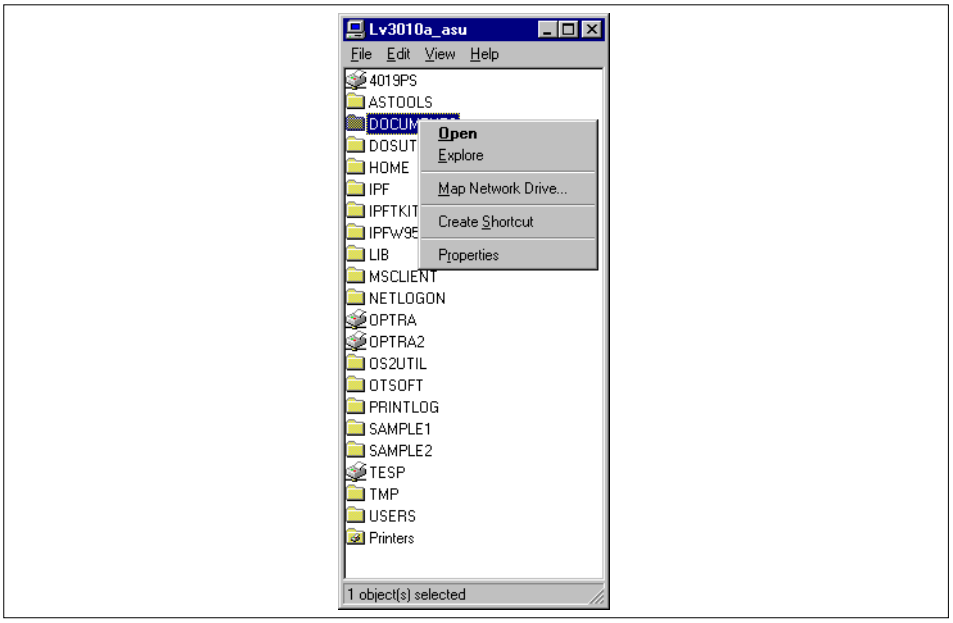


Figure 221. List of AS/U Resources

4. Select the **Map Network Drive...** menu item.
5. A window appears (see Figure 222). A default drive mapping will have been given, though this can be changed. You also have the option of selecting whether the drive is automatically attached during logon (a password will be required if the current user logged on to Windows NT is not an AS/U user).

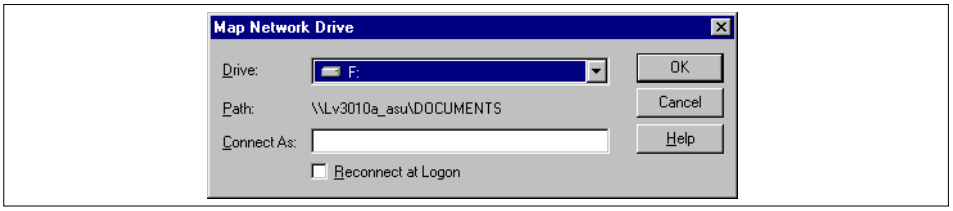


Figure 222. Map Network Drive

6. Click on **OK**.

A drive mapping is made. You can view this by looking in My Computer on the desktop (seeFigure 223).

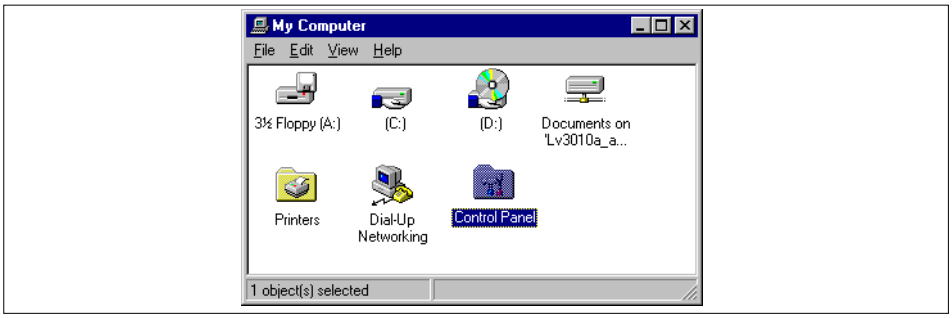


Figure 223. My Computer

6.17.2 Sending Messages to Clients

A message can be sent to a Windows NT client by using the net command:

```
net send lv3010k "Hello lv3010k"
```

This presents a window on the Windows NT system (as shown in Figure 224).

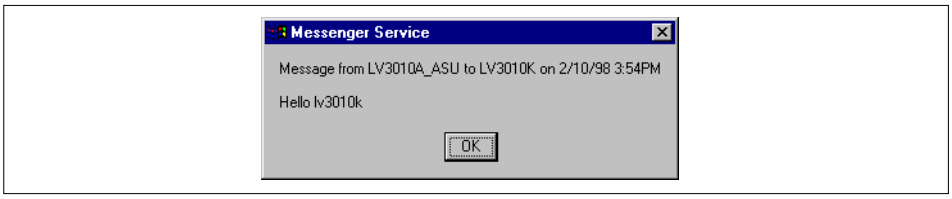


Figure 224. Sending a Message to a Client

6.17.3 Time Synchronization

The date and time on a Windows NT system can be set from the AS/U server:

1. Log on as **administrator** on the local Windows NT system in the AS/U domain.
2. Select the **Start** icon and select **Run** or open a **Command window**.
3. Type the command (if lv3010a_asu is the AS/U server):

   ```
   net time \\lv3010a_asu /set /yes
   ```

This synchronizes the local Windows NT clock with the AS/U server.

6.17.4 File Names

AS/U shared directories, by default, do not support mixed-case for file and directory names. Any file or directories containing uppercase letters will not be viewable by client systems. This is because Windows NT does not distinguish between upper- and lowercase characters. Users could get confused if two files on the server have the same name but in different cases. The files would be viewable on the Windows NT system but the user would not be able to specify which file they were accessing.

Mixed case support can be enabled for all shared file systems on AS/U by editing the MixedCaseSupport registry option for FileServiceParameteres. The default is `0`, but setting to `1` enables mixed case:

```
regconfig SYSTEM/CurrentControlSet/Services/AdvancedServer\
/FileServiceParameters MixedCaseSupport REG_DWORD 1
```

After making the registry change, restart AS/U for the change to become effective.

The AS/U documentation states that this change may degrade performance of the server. In addition, as problems can arise with file names having the same name but different case, this option should be used with caution.

6.17.5 Mounting Shared NT Directories

While AS/U doesn't provide client tools to connect to remote Windows NT servers and workstations, it does provide a utility, `lmshell`, that emulates a client MS-DOS session. By using this `lmshell` command, files can be copied from remote Windows NT systems to the AS/U server.

The following screen shows a session on the AS/U server connecting to a remote Windows NT systems, lv3010f, that has a shared directory called tools. The tools directory has a file called test.out that we want to copy:

```
# lmshell
C:\TMP> net use d: \\lv3010f\tools
        D: linked to \\LV3010F\TOOLS
C:\TMP> d:
D:\> dir
  Volume in drive D LV3010F Directory of .

IMAGES        <DIR>      2-16-98   2:16p
TEST     OUT     2186    2-23-98   5:14p

       2File(s)  8028160 bytes free

D:\> copy test.out c:\tmp\test.out
    1 File copied
D:\> exit
#
```

6.17.6 Password Encryption

AS/U can handle passwords passed by clients that are in plain text or encrypted. This means that Windows NT 4.0 clients will still be able to log in after applying Service Pack 3.

6.17.7 Year 2000

AS/U is year 2000 compliant since it uses UNIX, Windows NT and DOS times, which are all year 2000 ready.

Chapter 7. Samba for UNIX

Samba is a suite of programs that work together to allow clients to access a server's filespace and printers via the SMB (Server Message Block) protocol. Initially written for UNIX, Samba now also runs on NetWare, OS/2 and VMS.

In this chapter we use an RS/6000 running AIX 4.2.1 as the server and a PC running Windows NT 4.0 as the client. We also tested AIX 4.1.4 and 4.3. Everything worked the same as on the AIX 4.2.1 server.

7.1 Samba Overview

Samba enables UNIX systems to act as servers for PC client systems running MS-DOS, OS/2, Windows, Windows for Workgroups, Windows 95 and Windows NT. Samba implements the Server Message Block (SMB) protocol that enables clients and servers to exchange messages and data. Windows NT, Windows 95, OS/2 Warp Connect and OS/2 Warp 4 clients do not need any extra software to access a Samba server. These operating systems all come with TCP/IP, which is all that is needed to access the Samba server.

The version tested for this redbook was Version 1.9.18p1. Samba is distributed via anonymous FTP. Samba is available free of charge according to the rules of the GNU Public License. The definitive source for the code, documentation, license information and patches is available on the Web at the following URL:

```
http://samba.anu.edu.au
```

Samba is distributed in source form. You must compile the source files once you FTP them to your system. Precompiled binaries are available for some UNIX types and can be downloaded from the following address:

```
ftp://samba.anu.edu.au/pub/samba/Binary_Packages
```

Be aware that the precompiled binaries may not be the latest version and you also give up the option to define custom options in the makefile that apply to your environment.

Samba is distributed and supported via the Internet. The Web site and newsgroup are listed below:

```
http://samba.anu.edu.au/samba
```

```
comp.protocols.smb
```

The Web site and newsgroup are the primary sources of support and how-to information. There is also a mailing list to which you can subscribe if you prefer to receive e-mail notification of new Samba information. You can subscribe to the mailing list by sending e-mail to `samba@listproc.anu.edu.au`. Leave the subject line of the e-mail blank and enter the following text in the body of the email:

```
subscribe samba Firstname Lastname

subscribe samba-announce Firstname Lastname
```

Substitute your first and last name for `Firstname` and `Lastname`.

The full set of Samba documentation is installed in a location specified in the makefile. This default is /usr/local/samba/doc.

7.2 Installation

In this section we discuss the installation steps. The specific configuration steps will be detailed in the next section. You will need to know how to FTP a file via the Internet, uncompress and extract a file using the `tar` command, modify a makefile, and compile the source to create the binaries necessary to run Samba.

If you have downloaded the precompiled binaries, go directly to 7.3, “Configuration” on page 282.

7.2.1 Downloading and Installing Samba Code

The first step in the installation is to FTP the Samba distribution to your system. You will have a compressed file that you must uncompress and then extract, using the standard UNIX `tar` command. A directory is created in the same directory to which you transferred the image. In the following example, the Samba distribution is a file named samba-1.9.18p1.tar and the directory it was downloaded to is /usr/local/download. You must have the necessary permissions to perform the download, uncompress the file and perform the compilation. You must be logged on as root to perform some parts of the Samba installation. Your system also must have a C compiler installed. The server hostname for the installation described here is itsonice.

```
$ls -la
total 9744
drwxr-sr-x   3 root     sys 512 Jan 26 14:48 .
drwxr-sr-x   6 sys      sys 512 Jan 27 09:02 ..
drwxr-sr-x   6 1002     1002 512 Jan 12 12:45 samba-1.9.18p1
-rw-r--r--   1 root     sys 4976640 Jan 26 14:43 samba-1.9.18p1.tar
[root@itsonice]/usr/local/download
```

After extracting the distribution file using the `tar` command, a directory named /usr/local/download/samba-1.9.18p1 was created.

In our example, the source files reside in the directory /usr/local/download/samba-1.9.18p1/source, which is created by running the `tar` command. The makefile also resides in this directory. The following screen shows the part of the makefile with the AIX information.

```
# This is for AIX 4.x
# contributed by tomc@osi.curtin.edu.au
# FLAGSM = -DAIX -DFAST_SHARE_MODES
# LIBSM =
# This is for AIX 4.x with quota support
# contributed by tomc@osi.curtin.edu.au
FLAGSM = -DAIX -DFAST_SHARE_MODES -DQUOTAS
LIBSM =
# This is for AIX 3.2.5 with DCE/DFS
# contributed by Jim Doyle <doyle@oec.com>
# FLAGSM = -DAIX -DDFS_AUTH -DSIGCLD_IGNORE -DNO_SIGNAL_TEST
# LIBSM = -lc_r -ldce -lpthreads
# CC = cc_r
# LIBSM = -lc_r -ldce -lpthreads
# CC = cc_r
```

For our test, we uncommented the section for AIX 4.x with quota support. As you can see, there is also a section for AIX 4.x without quota support and a section for AIX 3.2.5. Be sure to only uncomment one section.

Now run the `make` command to create the binaries. After the `make` runs successfully, run `make install` to install the binaries and man pages. By default, the Samba distribution is installed in /usr/local/samba. This may be changed in the makefile at compile time, if necessary.

7.2.2 Configuring the Samba Daemons

At this point, Samba is installed on your system. Let's see now how to configure the two daemons that are the base of the Samba product, smbd and nmbd. The smbd process provides LAN Manager-like services to clients

using the SMB protocol. The nmbd process provides NetBIOS name server support to clients. They can either be started as daemons in a start up script, for example in /etc/rc.local, or they can be started by inetd. Choose only one method of starting Samba. If you chose to use inetd, appropriate entries must be made in /etc/services and /etc/inetd.conf. Ensure that the default port for samba is not used by any other program. The default port is port 139, it should be used if possible, though any port may be used. Ensure that a line similar to the following is in /etc/services:

```
netbios-ssn 139/tcp
```

The following is a fragment of the /etc/services file from our server:

```
profile         136/tcp                         # PROFILE Naming System
profile         136/udp                         # PROFILE Naming System
netbios-ns      137/tcp                         # NETBIOS Name Service
netbios-ns      137/udp                         # NETBIOS Name Service
netbios-dgm     138/tcp                         # NETBIOS Datagram Service
netbios-dgm     138/udp                         # NETBIOS Datagram Service
netbios-ssn     139/tcp                         # NETBIOS Session Service
netbios-ssn     139/udp                         # NETBIOS Session Service
emfis-data      140/tcp                         # EMFIS Data Service
emfis-data      140/udp                         # EMFIS Data Service
emfis-cntl      141/tcp                         # EMFIS Control Service
emfis-cntl      141/udp                         # EMFIS Control Service
```

Now put a suitable line in the file /etc/inetd.conf, such as the following:

```
netbios-ssn stream tcp nowait root /usr/local/samba/bin/smbd
```

The following is a fragment of the /etc/inetd.conf file from our server:

```
echo    stream  tcp     nowait  root    internal
discard stream  tcp     nowait  root    internal
chargen stream  tcp     nowait  root    internal
daytime stream  tcp     nowait  root    internal
time    stream  tcp     nowait  root    internal
echo    dgram   udp     wait    root    internal
discard dgram   udp     wait    root    internal
chargen dgram   udp     wait    root    internal
daytime dgram   udp     wait    root    internal
time    dgram   udp     wait    root    internal
## The following line is for installing over the network.
#instsrv stream tcp     nowait  netinst /u/netinst/bin/instsrv instsrv -r /tmp/n
etinstalllog /u/netinst/scripts
dtspc   stream  tcp     nowait  root    /usr/dt/bin/dtspcd /usr/dt/bin/dtspcd
#imap2  stream  tcp     nowait  root    /usr/sbin/imapd imapd
#pop3   stream  tcp     nowait  root    /usr/sbin/pop3d pop3d
cmsd    sunrpc_udp      udp     wait    root    /usr/dt/bin/rpc.cmsd cmsd 100068
 2-5
ttdbserver      sunrpc_tcp      tcp     wait    root    /usr/dt/bin/rpc.ttdbserv
er rpc.ttdbserver 100083 1
netbios-ssn stream tcp nowait root /usr/local/samba/bin/smbd smbd
```

Starting Samba using a script will cause the server to always be available for client requests. Therefore, starting a client session may be faster. Starting the server using inetd may be slower but you will conserve system memory and you may be able to provide additional security by using utilities such as the tcpd TCP wrapper. Also, if for any reasons one of these daemons has to die, it would be restarted automatically at the next request from a client.

7.2.3 Creating a Minimum Configuration File

For the smbd and nmbd daemons to run, you need to provide them with a configuration file. The default location for this file is /usr/local/samba/lib and its name is smb.conf. There is an example of this smb.conf file in the /usr/local/download/samba-1.9.18p1/examples directory. In 7.3, “Configuration” on page 282, we discuss how to customize this file for your environment. However, using the default configuration file, you should be able to test your configuration.

The following is a sample of this default configuration file:

```
# This is the main Samba configuration file. You should read the
# smb.conf(5) manual page in order to understand the options listed
# here. Samba has a huge number of configurable options (perhaps too
# many!) most of which are not shown in this example
#
# Any line which starts with a ; (semi-colon) or a # (hash)
# is a comment and is ignored. In this example we will use a #
# for commentry and a ; for parts of the config file that you
# may wish to enable
#
# NOTE: Whenever you modify this file you should run the command
# "testparm"
# to check that you have not many any basic syntactic errors.
#
#======================= GlobalSettings=========================
[global]

# workgroup = NT-Domain-Name or Workgroup-Name, eg: REDHAT4
   workgroup = ITSOAUSNT

# server string is the equivalent of the NT Description field
   server string = Samba Server(RS3010)
```

We modified it slightly to reflect our environment. We set ITSOAUSNT as our domain name and Samba Server (RS3010) as our identifier. Refer to 7.3, “Configuration” on page 282 for further customization.

7.2.4 Checking the Samba Installation

There are two elements you may need to verify to ensure that you have correctly installed and configured Samba product. The first one is checking that the smb.conf file is correct, the second is that your machine is now acting as an SMB server.

7.2.4.1 Checking the smb.conf File

Once the smb.conf file is modified to reflect your environment, you should run the test program provided to test if the smb.conf file is valid. The program is /usr/local/samba/bin/testparm. If this program runs without errors, you have a valid smb.conf file. The following is an example of the screen output of the testparm program.

```
$testparm
Load smb config files from /usr/local/samba/lib/smb.conf
Unknown parameter encountered: "domain controller"
Ignoring unknown parameter "domain controller"
Processing section "[homes]"
Processing section "[tmp]"
Processing section "[sgardner]"
Processing section "[foo]"
Processing section "[residency]"
Processing section "[printers]"
Global parameter load printers found in service section!
Processing section "[printers]"
Global parameter load printers found in service section!
Processing section "[printers]"
Global parameter load printers found in service section!
Loaded services file OK.
```

Notice the final line of output displays `Loaded services file OK`. This is your indication that the smb.conf file is valid.

7.2.4.2 Checking Your Server

If your machine is correctly installed and configured, it is now able to act as an SMB server and provide information about the shares available. The command used to obtain the information is `smbclient`, as shown below.

```
/usr/local/bin/smbclient -L yourhostname
```

If this command shows a list of the resources you configured in smb.conf, you have a properly-running Samba server. Now you should be able to access the shared resources from your clients.

The following screen shows the result of the `smbclient -L` command on our server named itsonice. We see information such as the domain, the operating system, the version of Samba being run and the devices that have been set up to be shared with clients.

```
$ smbclient -L itsonice
Unknown parameter encountered: "domain controller"
Ignoring unknown parameter "domain controller"
No interface found for address 9.3.1.72
Added interface ip=9.3.1.72 bcast=9.255.255.255 nmask=255.0.0.0
Server time is Wed Mar 18 14:40:35 1998
Timezone is UTC-6.0
Password:
Domain=[ITSOAUSNT] OS=[Unix] Server=[Samba 1.9.18p1]
security=user

Server=[ITSONICE] User=[root] Workgroup=[ITSOAUSNT] Domain=[ITSOAUSNT]

        Sharename      Type      Comment
        ---------      ----      -------
        4312ps         Printer   IBM Network printer in Steve's office
        draft          Printer   IBM 3130 in Lab Print Room
        final          Printer   Lexmark Optra N in Lab Print Room
        foo            Disk
        homes          Disk
        IPC$           IPC       IPC Service (Samba Server(RS3010))
        printers       Printer   All Printers
        residency      Disk      Public Residency Data
        root           Disk      Home directory of root
        sgardner       Disk      sgardner home
        tmp            Disk      temporary files

NOTE: There were share names longer than 8 chars.
On older clients these may not be accessible or may give browsing errors


This machine has a browse list:

        Server               Comment
        ---------            -------
        ALEXGTP
        BARCELONA            OOAD NETSTATION Samba Server
        BJ2225A
```

When the `testparm` command and `smbclient` command return positive results and the smbd process is running, you should have a properly-functioning Samba server.

The next section discusses the unique configuration options you can define in the smb.conf file to address the needs of your environment. It is mainly an extract of the /usr/local/samba/doc/smb.conf.5 file.

7.3 Configuration

For configuring Samba, there is no fancy user interface and no complicated command line procedures. Almost everything is done by editing one file, the

smb.conf file. The default location for this file is /usr/local/samba/lib/smb.conf, but once more, this can be changed at compile time. The smb.conf file is made up of runtime configuration information used by the smbd process.

The file format is made up of sections and parameters defined in those sections. Each section has a name between square brackets. The parameters for a section have the syntax `name = value`. A section continues until another name in square brackets is found. The section and parameter names are not case-sensitive. Each new line in the file is either a comment, section or parameter. Lines of white space only and lines beginning with semi-colons are ignored.

The following is a set of very useful variables that you can use in this configuration file:

%S The name of the current service, if any.

%P The root directory of the current service, if any.

%u User name of the current service, if any.

%g Primary group name of %u.

%U Session user name (the user name that the client wanted, not necessarily the same as the one they got).

%G Primary group name of %U.

%H The home directory of the user given by %u.

%v The Samba version.

%h The hostname on which Samba is running.

%m The NetBIOS name of the client machine (very useful).

%L The NetBIOS name of the server. This allows you to change your configuration based on what the client calls you.

%M The Internet name of the client machine.

%d The process ID of the current server process.

%a The architecture of the remote machine. Only some are recognized, and those may not be 100 percent reliable. It currently recognizes Samba, WfWg, WinNT and Win95. Anything else is UNKNOWN.

%I The IP address of the client machine.

%T The current date and time.

The following is an example of a section from the smb.conf file.

```
#====================== Global Settings ===================================
[global]

# workgroup = NT-Domain-Name or Workgroup-Name, eg: REDHAT4
   workgroup = ITSOAUSNT

# server string is the equivalent of the NT Description field
   server string = Samba Server(RS3010)

# This option is important for security. It allows you to restrict
# connections to machines which are on your local network. The
# following example restricts access to two C class networks and
# the "loopback" interface. For more examples of the syntax see
# the smb.conf man page
;   hosts allow = 192.168.1. 192.168.2. 127.

# If you want to automatically load your printer list rather
# than setting them up individually then you'll need this
   printcap name = /etc/sambaprt
   load printers = yes
```

There are three special sections. They are named global, homes, and printers. Let's have a closer look to them.

7.3.1 Populating the Global Section

This section is used to defined global parameters that describe our Samba server, or default values that will be set for every service defined later. Each of these services may override the default in its own section.

Let's start with a minimum configuration. We need to indicate the name of the NT domain or the workgroup in which we want to include our Samba server, This is done using the workgroup parameter:

workgroup This controls what workgroup in which your server will appear to be when queried by clients.

Default:
`set in the makefile`

Example:
`workgroup = ITSOAUSNT`

At this point we have a running samba server, but we can control how this server will announce itself to the clients on the network with several other parameters:

server string This controls what string will show up in the printer comment box in the print manager and next to the IPC connection in "net view". It can be any string that you want to show your users. It also sets what will appear in browse lists next to the machine name.

Default:
```
server string = Samba %v
```

Example:
```
server string = ITSO Samba server
```

announce as This specifies what type of server nmbd will announce itself as in browse lists. By default this is set to Windows NT. The valid options are `NT`, `Win95` or `WfW`, meaning Windows NT, Windows 95 and Windows for Workgroups respectively. Do not change this parameter unless you have a specific need to stop Samba appearing as an NT server. Doing so may prevent Samba servers from correctly participating as browser servers.

Default:
```
announce as = NT
```

Example:
```
announce as = Win95
```

announce version This specifies the major and minor version numbers that nmbd uses when announcing itself as a server. The default is 4.2. Do not change this parameter unless you have a specific need to set a Samba server to be a downlevel server.

Default:
```
announce version = 4.2
```

Example:
```
announce version = 2.0
```

The next area where you can change the defaults parameters is the default configuration of Samba itself, starting with the configuration file name:

config file This allows you to override the configuration file to use, instead of the default (usually smb.conf). It may seem strange to put the name of the configuration file in the

configuration file, but it can be very useful. If during the parsing of the file this parameter is found, the process then jumps to the new file specified and continues in sequence. This allows you to specify the configuration file to use based on the name of the client or the name of the user, if you use the special variables in the file name. If the specified file doesn't exist, the process will continue parsing the current file.

Example:

```
config file = /usr/local/samba/lib/smb.conf.%m
```

This will call the file /usr/local/samba/lib/smb.conf.lv3010j if the name of the client requesting access is lv3010j.

include This one is very similar. It allows you to include one configuration file inside another. The file is included literally, as though typed in place.

debug level The value of the parameter (an integer) allows the debug level (logging level) to be specified in the smb.conf file. This is to give greater flexibility in the configuration of the system. The default will be the debug level specified at the command line.

Example:

```
debug level = 3
```

log file This options allows you to override the name of the Samba log file (also known as the debug file). This option takes the standard substitutions, allowing you to have separate log files for each user or machine.

Example:

```
log file = /usr/local/samba/var/log.%m
```

The last area we are going to describe is the networking role that our Samba server can play. First, we can specify which network and which machine we want to serve:

interfaces This option allows you to set up multiple network interfaces, so that Samba can properly handle browsing on all interfaces. The option takes a list of ip/netmask pairs. The netmask may either be a bitmask or a bitlength.

For example, the following line:

```
interfaces = 192.168.2.10/24 192.168.3.10/24
```

would configure two network interfaces with IP addresses 192.168.2.10 and 192.168.3.10. The netmasks of both interfaces would be set to 255.255.255.0. You could produce an equivalent result by using:

```
interfaces = 192.168.2.10/255.255.255.0
192.168.3.10/255.255.255.0
```

if you prefer that format. If this option is not set then Samba will attempt to find a primary interface, but won't attempt to configure more than one interface.

allow hosts

A synonym for this parameter is hosts allow. This parameter is a comma-delimited set of hosts that are permitted to access the server. You can specify the hosts by name or IP number. For example, you could restrict access to only the hosts on a Class C subnet with a line such as `allow hosts = 150.203.5`. You can also specify hosts by network/netmask pairs and by netgroup names, if your system supports netgroups. The EXCEPT keyword can also be used to limit a wildcard list. The following examples may provide some help:

Example 1 - Allow all IPs in 150.203.*.* except one:

```
hosts allow = 150.203. EXCEPT 150.203.6.66
```

Example 2 - Allow hosts that match the given network/netmask:

```
hosts allow = 150.203.15.0/255.255.255.0
```

Example 3 - Allow two hosts:

```
hosts allow = lapland, arvidsjaur
```

Example 4 - Only allow hosts in netgroup foonet or localhost, but deny access from one particular host:

```
hosts allow = @foonet, localhost
hosts deny = pirate
```

Note that access still requires suitable user-level

passwords.

See testparm(1) for a way of testing your host access to see if it does what you expect.

Default:
None (that is, all hosts permitted access)

deny hosts This is the opposite of allow hosts; hosts listed here are NOT permitted access to services unless the specific services have their own lists to override this one. Where the lists conflict, the allow list takes precedence.

Default:
None (that is, no hosts specifically excluded)

domain master This makes our Samba server the domain master browser. It will collects the information from any local master browser on subnets and provide them with the full list it has collected. You should only have one domain master browser in each domain.

Default:
`domain master = no`

local master This option allows the nmbd to become a local master browser on a subnet. If set to False, then nmbd will not attempt to become a local master browser on a subnet and will also lose in all browsing elections. By default, this value is set to true. Setting this value to true doesn't mean that Samba will become the local master browser on a subnet, just that the nmbd will participate in elections for the local master browser.

Default:
`local master = yes`

preferred master This boolean parameter controls if Samba is a preferred master browser for its workgroup. If this is set to true, on start up, Samba will force an election and it will have a slight advantage in winning the election. It is recommended that this parameter is used in conjunction with `domain master = yes`, so Samba can guarantee becoming a domain master.

Use this option with caution, because if there are several hosts (whether Samba servers, Windows 95 or NT) that are preferred master browsers on the same subnet, they will each periodically and continuously attempt to become the local master browser.This will result in unnecessary broadcast traffic and reduced browsing capabilities.

Default:
`preferred master = no`

wins server This specifies the DNS name (or IP address) of the WINS server with which Samba should register. If you have a WINS server on your network, you should set this to the WINS servers name.

Point this at your WINS server if you have a multi-subnetted network.

Default:
`wins server =`

wins proxy This is a boolean that controls if nmbd will respond to broadcast name queries on behalf of other hosts. You may need to set this to no for some older clients.

Default:
`wins proxy = no`

With these parameters you should be able to customize the global section of the configuration to adapt to your needs. Now let's see how to declare and share resources.

7.3.2 Populating the Homes Section

If a section called [homes] is included in the configuration file, services connecting clients to their home directories can be created on the fly by the server. When the connection request is made, the existing services are scanned. If a match is found, it is used. If no match is found, the requested service name is treated as a user name and looked up in the local passwords file. If the name exists and the correct password has been given, a service is created by cloning the [homes] section. Let's now see some of the parameters that apply to this section:

comment

This is a text field that is seen next to a share when a client does a net view to list what shares are available.

Default:
No comment string

Example:
```
comment = Fred's Files
```

path

This parameter specifies a directory to which the user of the service is given access. In this [homes] section, you would normally use the variables to specify the directory for the user who accesses your server. Note that this path will be based on root dir if one was specified.

Default:
None

Example:
```
path = /home/%u
```

browseable

This controls whether this share is seen in the list of available shares in a net view or browse list.

Default:
```
browseable = Yes
```

Example:
```
browseable = No
```

writable

A synonym for this parameter is write ok, and one antonym is read only.

If this parameter is `no`, then users of a service may not create or modify files in the service's directory.

Default:
```
writable = no
```

Examples:
```
read only = no
writable = yes
```

create mask

When a file is created, the necessary permissions are calculated according to the mapping from the DOS

modes to UNIX permissions. The resulting UNIX mode is then bit-wise ANDed with this parameter. This parameter may be thought of as a bit-wise MASK for the UNIX modes of a file. Any bit *not* set here will be removed from the modes set on a file when it is created.

The default value of this parameter removes the group and other write and execute bits from the UNIX modes. Following this Samba will bit-wise OR the UNIX mode created from this parameter with the value of the force create mode parameter that is, by default, set to 000.

Default:
`create mask = 0744`

Example:
`create mask = 0775`

hide dot files This is a boolean parameter that controls whether files starting with a dot appear as hidden files.

Default:
`hide dot files = yes`

Example:
`hide dot files = no`

valid users This is a list of users that should be allowed to log into this service. A name starting with @ is interpreted as a UNIX group.

If this is empty (the default) then any user can log in. If a username is in this list and the invalid users list, then access is denied for that user.

Default:
No valid users list (anyone can log in)

Example:
`valid users = greg, @pcusers`

invalid users This is a list of users that should not be allowed to log into this service. A name starting with @ is interpreted as a UNIX group.

Default:
No invalid users

Example:
```
invalid users = root fred admin @whee
```

max connections This option allows the number of simultaneous connections to a service to be limited. If max connections is greater than 0, then connections will be refused if this number of connections to the service are already open. A value of zero means an unlimited number of connections may be made.

Record lock files are used to implement this feature. The lock files will be stored in the directory specified by the lock directory option.

Default:
```
max connections = 0
```

Example:
```
max connections = 10
```

The following is an example of what a usual [homes] section looks like. It shows that the comment line you will see related to the share is the home directory for your particular user, that no one except you will be able to browse it, that you can write and delete files in this share, that the path for this share is /home/itso/yourusername and that the creation mask is set to 0755.

```
#========================== Share Definitions ==========================
[homes]
   comment = Home Directory for %u
   browseable = no
   writable = yes
   path = /home/itso/%u
   create mask = 0755
```

7.3.3 Populating the Printers Section

If a section called [printers] exists, it works like [homes], but for printers. If a [printers] section occurs in the configuration file, users are able to connect to any printer specified in the local host's printcap file. When a connection request is made, the existing services are scanned. If a match is found, it is used. If no match is found, but a [homes] section exists, it is used as described above. Otherwise, the requested service name is treated as a printer name and the appropriate printcap file, or /etc/qconfig file in AIX, is scanned to see if the requested service name is a valid printer name. If a match is found, a new service is created by cloning the [printers] section. Here are some of the useful parameters that you can change for your environment:

printcap name This parameter is used to override the compiled default printcap name used by the server (usually /etc/qconfig for AIX). You can also specify `printcap name = lpstat`, though the result on the client is unusual, since you have a mix of printer names and headers for the `lpstat -v` command. If you want to limit the access from your network client to a specific printer, you can overwrite the default printcap name to a specific file. The following is an example of the minimal printcap file:

```
print1|My Printer 1
print2|My Printer 2
```

where the `|` separates aliases of a printer. The fact that the second alias has a space in it gives a hint to Samba that it's a comment.

Default:

```
printcap name = /etc/printcap
```

Example:

```
printcap name = /etc/myprintcap
```

print command After a print job has finished spooling to a service, this command will be used via a system call to process the spool file. Typically, the command specified will submit the spool file to the host's printing subsystem, but there is no requirement that this be the case.The server will not remove the spool file, so whatever command you specify should remove the spool file when it has been processed, otherwise you will need to manually remove old spool files.

The print command is simply a text string. It should be used verbatim, with two exceptions: All occurrences of `%s` will be replaced by the appropriate spool file name, and all occurrences of `%p` will be replaced by the appropriate printer name. The spool file name is generated automatically by the server, the printer name is discussed below.

The full path name is used for the file name if `%s` is not preceded by a `/`. Any occurrences of %f get replaced by the spool filename without the full path at the front.

The print command MUST contain at least one occurrence of `%s` or `%f`; the `%p` is optional. At the time a job is submitted, if no printer name is supplied, the `%p` is silently removed from the printer command.

Default:
`print command = lpr -r -P %p %s`

Example:
`print command = /usr/local/samba/bin/myprintscript %p %s`

printer

This parameter specifies the name of the printer to which print jobs spooled through a printable service will be sent.

Default:
None

Example:
`printer name = laserwriter`

printing

This parameter controls how printer status information is interpreted on your system, and also affects the default values for the `print`, `lpq`, and `lprm` commands.

Currently, six printing styles are supported. They are `printing = bsd`, `printing = sysv`, `printing = hpux`, `printing = aix`, `printing = qnx` and `printing = plp`.

Use the testparm program to see what the defaults are

for the other print commands when you use these three options.

Example:
`printing = aix`

printable If this parameter is yes, then clients may open, write to and submit spool files on the directory specified for the service.

Note that a printable service will ALWAYS allow writing to the service path (user privileges permitting) via the spooling of print data. The read only parameter controls only non-printing access to the resource.

Default:
`printable = no`

Example:
`printable = yes`

path This is where print data will spool before being submitted to the host for printing.

postscript This parameter forces a printer to interpret the print files as postscript. This is done by adding a `%!` to the start of print output.

This is useful when you have lots of PCs that persist in putting a control-D at the start of print jobs, which confuses your printer.

Default:
`postscript = False`

Example:
`postscript = True`

The following is an example of what a typical [printers] section looks like. It shows the comment that appears in the browse list, the directory where the print files are spooled, the authorization for anyone to see the printer in the browse list and the indication that you cannot write to the /usr/spool/samba directory unless you use a print command.

```
[printers]
   comment = All Printers for server %h
   path = /usr/spool/samba
   browseable = yes
   writable = no
   printable = yes
   print command = /usr/local/samba/bin/myprintscript %s %p
```

7.3.4 Defining Your Own Service

Sections other than the three special sections can be created. These are referred to as normal sections. Each section describes a service. A service consists of a directory that is given access, plus a description of the access rights that are granted to the user of the service. Some housekeeping options may also be specified. Services are either filespace services (used by the client as an extension of their native file systems) or print services (used by the client to access print services on the host running the server). If a services is a guest service, a password is not required to access it. A specified guest account is used to define access privileges in this case.

The following example shows how to create a file system share, reserved for one user, that will access the share as read-only.

```
[fredsdir]
     comment = Fred's Service
     path = /home/fred/private
     browseable = no
     valid users = fred
     public = no
     writable = no
     printable = no
```

The following example shows how to create a printer for a very specific use. In this example, the printer allows the user to print a GIF file directly.

```
[GIFPRN]
     comment = Gif printer
     path = /usr/spool/samba
     printer = ps1
     public = yes
     writable = no
     printable = yes
     print command = cat %s | gif2ps | lpr -P%p && rm %s
```

There are many other examples of shares you can create in the smb.conf.default file. There are many options to use, so you should be able to find ones to suit your needs.

7.4 Accessing the Share Resources from the Client

Now that we have seen how to configure our server to create a share for our client, it is time to use the server.

7.4.1 Using the Graphical Interface

The easiest way to access our Samba server is by using the graphical interface. The first step is to locate our server in the Network Neighborhood. Double-click on the **Network Neighborhood** icon and then select **Entire Network**, then **Microsoft Windows Network**. The name of one or many domains or workgroups should appear (depending on the configuration of your site). Double-click on the icon to which the Samba server belongs. In our case, Figure 225 on page 298 shows our server in the ITSOAUSNT domain.

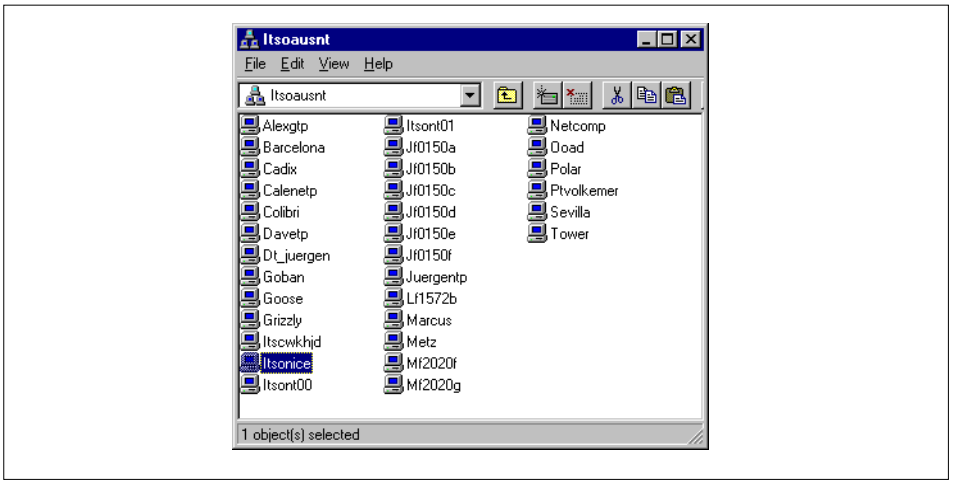


Figure 225. Location of Our Samba Server

By double-clicking on its name, we have a new window showing all browseable shares, as shown in Figure 226 on page 298.

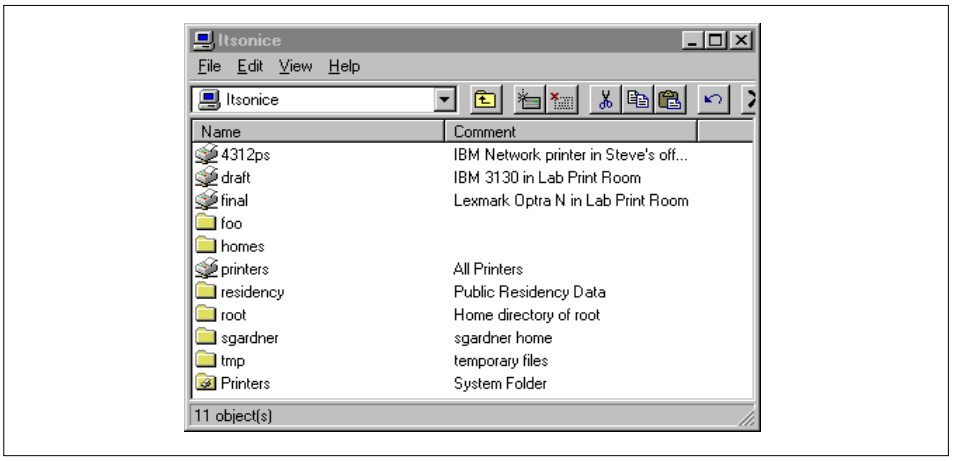


Figure 226. Detailed View of the Browseable Shares in the Samba Server

To map one of the directory as a network disk, right-click on the name of that directory and select **Map Network Drive...**, as shown in Figure 227 on page 299.

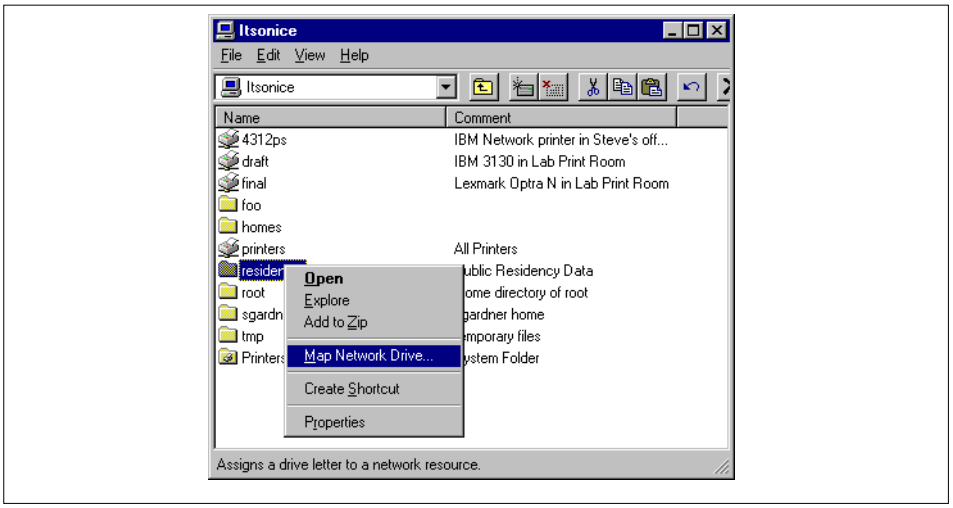


Figure 227. Mapping a Network Drive

Using a printable service is just as easy. Right-click on a printer name and select **Install** to be guided through the installation by a wizard, as shown in Figure 228 on page 299.

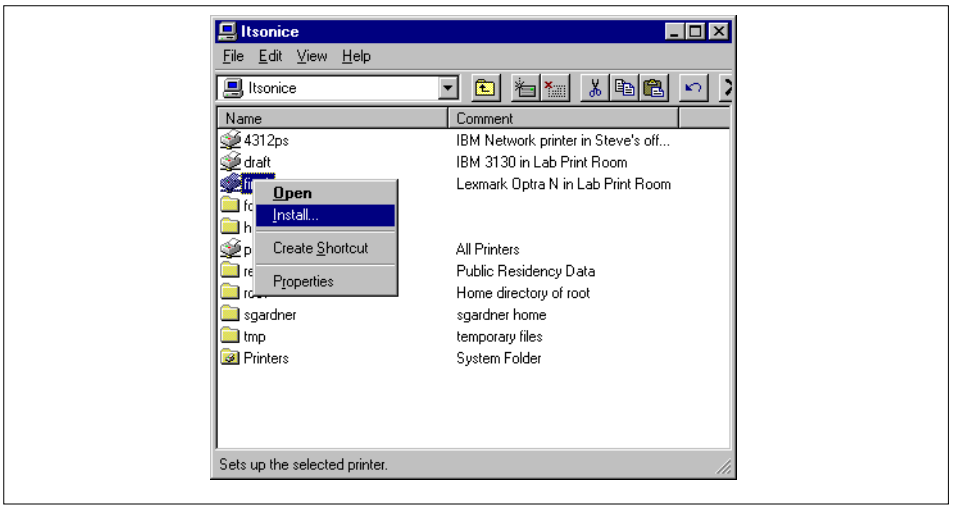


Figure 228. Adding a Remote Printer

If you cannot locate the Samba server in the browse list for your domain, use the find application to locate your Samba server. Start this application by clicking the **Start** button on the task bar, then **Find**, and **Find Computer...**.

Enter the name of your Samba server in the window, and after a moment, an icon representing your server should appear.

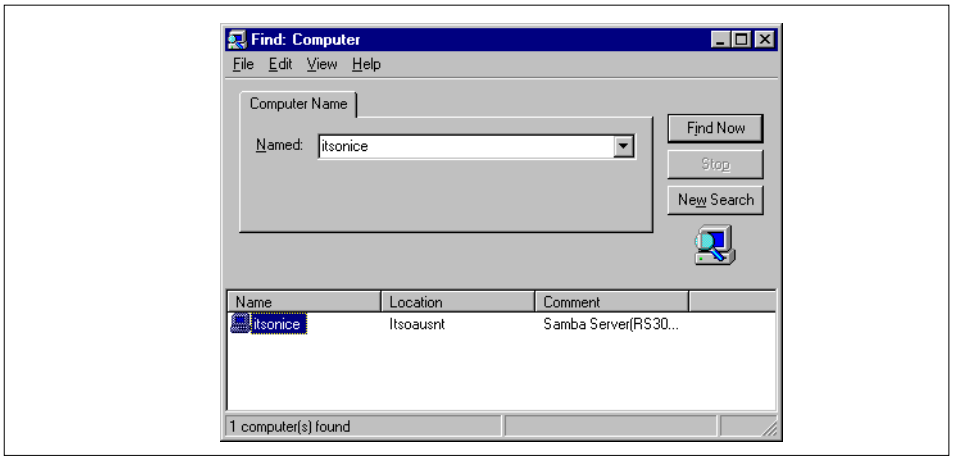


Figure 229. Using Find to Locate Your Server

Double-click on this icon and the window in Figure 226 on page 298 appears.

7.4.2 Using the Command Line

If you want to automate certain actions, you may prefer performing the same operations from the command line. The command that will help you locate, map and manage the share is the `net` command.

To list the shares available on your Samba server, use the `view` subcommand, as shown in Figure 230 on page 301

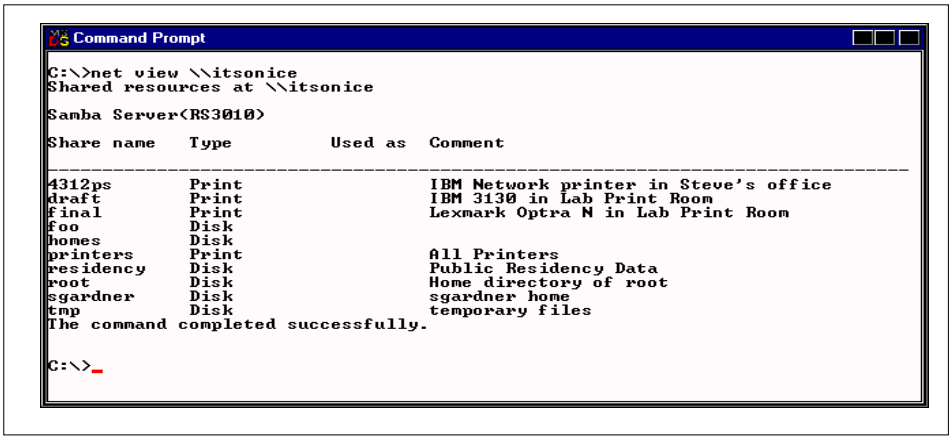


Figure 230. Listing the Shares Available from itsonice

When using the `net view` command to find a share, you must specify the `use` subcommand. Figure 231 on page 301 shows how to map the remote residency directory as drive `l:`:

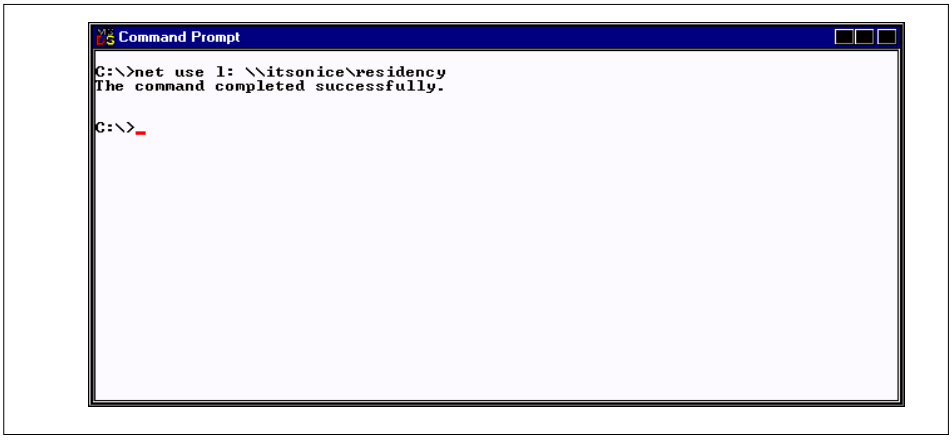


Figure 231. Using the net Command to Map a Network Drive

Use the same subcommand to map a line printer to a print queue on the server:

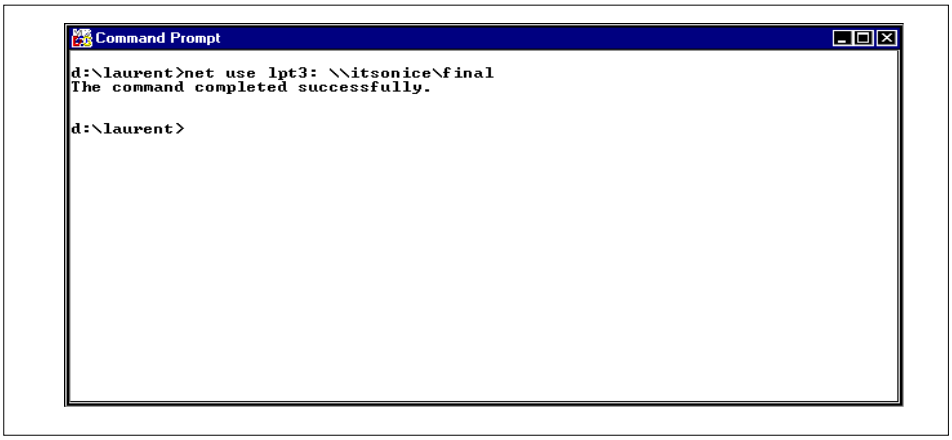


Figure 232. Mapping a Line Printer to a Remote Print Queue

An example of how to manage print jobs is shown in Figure 233. The first command output is the content of the queue, the second is the deletion of a job and the last one is the verification that the job has been removed.

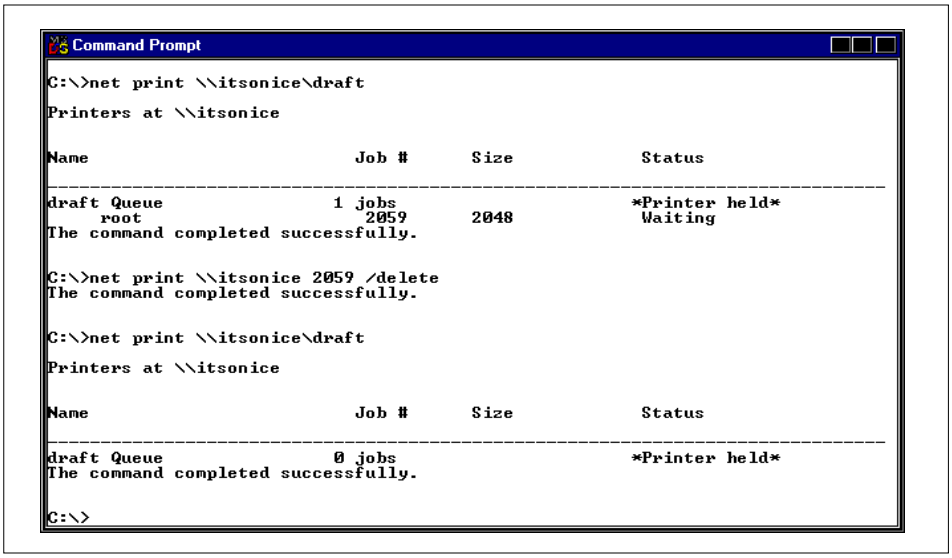


Figure 233. Print Job Management with the net Command

The last step is to remove the share you added to your system. Figure 234 shows how to disconnect a network drive.

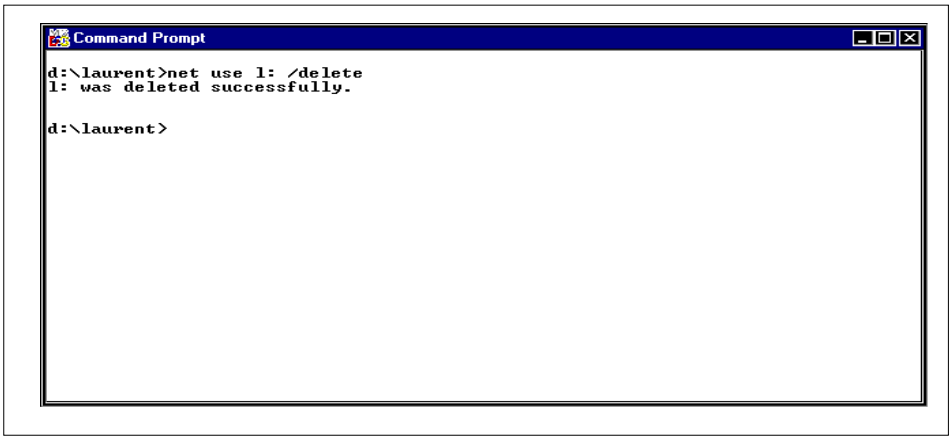


Figure 234. Removing a Network Drive with the net Command

Figure 235 shows how to remove the connection to a remote printer.

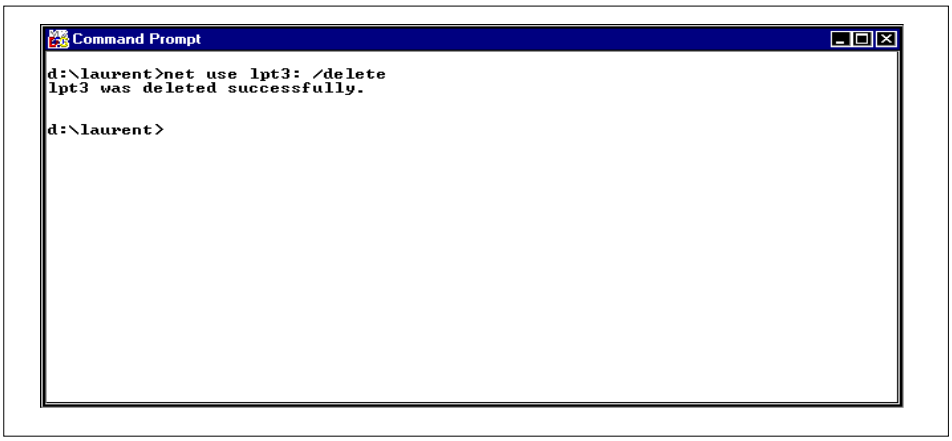


Figure 235. Deletion of a Line Printer

7.5 Using Samba to Back Up a Client

Samba offers a simple solution to back up the data you have on your Windows NT client. The `smbtar` command is part of the standard distribution and resides in he default /usr/local/samba/bin directory. It uses the standard tar format to back up the data to a file or a tape attached to the server.

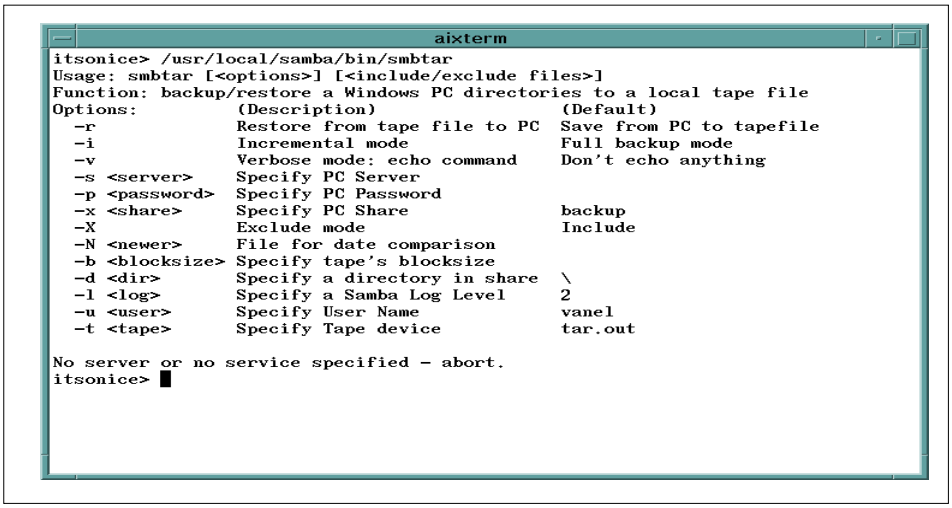


Figure 236. Options of the smbtar Command

As you can see, one of the elements of the `smbtar` command is the name of the share you want to back up. You then have to create a share resource on your Windows NT machine. To do so, select the directory you want to share and then edit its properties and select the sharing thumbnail. You should get a panel as shown in Figure 237. You must enter the name you want to give to this shared resource, the default is the name of the directory. Click on the **OK** button and your directory is now accessible from the network.

Figure 237. Sharing a Directory

To check that this resource is available, use the `smbclient` command. The following example shows that the residency directory is ready to be backed up.

```
# smbclient -L itsonice-U vanel
No interface found for address 9.53.62.117
Added interface ip=9.53.62.117 bcast=9.255.255.255 nmask=255.0.0.0
Server time is Fri Apr  3 11:52:13 1998
Timezone is UTC-6.0
Password:
Domain=[LV3010] OS=[Windows NT 4.0] Server=[NT LAN Manager 4.0]
security=user

Server=[ITSONICE] User=[] Workgroup=[ITSOAUSNT] Domain=[]

        Sharename      Type      Comment
        ---------      ----      -------
        IPC$           IPC       Remote IPC
        notes          Disk
        REPL$          Disk
        residency      Disk
        sauvegarde     Disk      test de sauvegarde

NOTE: There were share names longer than 8 chars.
On older clients these may not be accessible or may give browsing errors
```

We can now use the smbtar command to back up this directory. The following example shows the result of the smbtar command. You have to specify the name of the client with the -s option (here it is lv3010j), the name of the share with the -x option (here it is residency), the user used to connect to the client with the -u option (here it is administrator), and the name of the file or the tape drive you want to use for the backup (here it is backup.out). You can use the -p option on the command line to specify the password for the user administrator on the lv3010j machine, but for security reasons you may prefer to wait to be prompted before entering it. The option to specify the password on the command line may be useful if you want the automate the backup, at night for example.

```
# smbtar -v -s lv3010j -u administrator-x residency -t backup.out
server    is lv3010j
share     is residency\
tar args  is
tape      is backup.out
blocksize is
No interface found for address 9.53.62.117
Added interface ip=9.53.62.117 bcast=9.255.255.255 nmask=255.0.0.0
Server time is Fri Apr  3 12:04:54 1998
Timezone is UTC-6.0
Password:
Domain=[LV3010] OS=[Windows NT 4.0] Server=[NT LAN Manager 4.0]
security=user
getting file \entartreur.ram of size 43 bytes as a tar file entartreur.ram(4.19
22 kb/s) (average 4.19922 kb/s)
getting file \Minitel of size 40715 bytes as a tar file Minitel(364.777 kb/s) (
verage 334.477 kb/s)
getting file \test.class of size 2306 bytes as a tar file test.class(72.6436 kb
s) (average 280.365 kb/s)
tar: dumped 3 tar files
Total bytes written: 44032
```

Once your backup is finished, you can verify the result by using the standard UNIX `tar` command, as shown below:

```
# tar tvf backup.out
-rw-r--r--   0 0       43 Apr 01 17:29:34 1998 ./entartreur.ram
-rw-r--r--   0 0    40715 Apr 02 09:44:16 1998 ./Minitel
-rw-r--r--   0 0     2306 Mar 05 10:20:52 1998 ./test.class
#
```

Restoring the files to your client is just as easy. To do so, use the `-r` option, as shown below:

```
smbtar -v -r -s lv3010j -u administrator -x residency -t backup.out
server    is lv3010j
share     is residency\
tar args  is
tape      is backup.out
blocksize is
No interface found for address 9.53.62.117
Added interface ip=9.53.62.117 bcast=9.255.255.255 nmask=255.0.0.0
Server time is Fri Apr  3 12:25:27 1998
Timezone is UTC-6.0
Password:
Domain=[LV3010] OS=[Windows NT 4.0] Server=[NT LAN Manager 4.0]
security=user
restore tar file \entartreur.ram of size 43 bytes
restore tar file \Minitel of size 40715 bytes
restore tar file \test.class of size 2306 bytes
total of 3 tar files restored to share
#
```

7.6 Security Issues

The default behavior for Samba is to authenticate users using their AIX logon and password. When the users request access to a share, they are prompted with a window similar to the one shown in Figure 238.

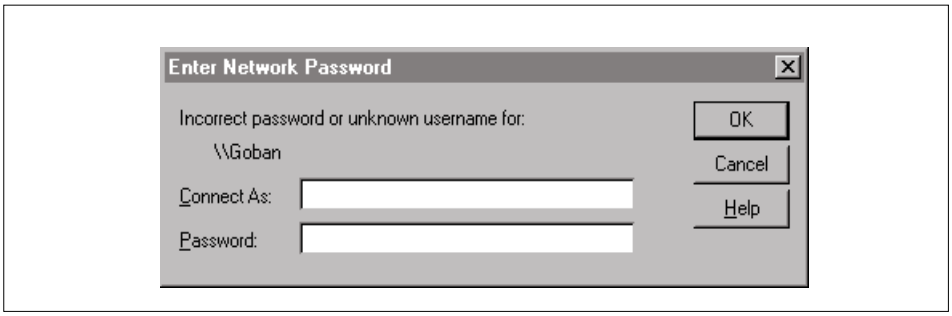


Figure 238. Request for Authentication Window

Users have to enter a valid UNIX login and password on the Samba server to get access to resources. With Windows NT Version 4, the logon and password are sent non-encrypted to the server. The server compares this information to the /etc/passwd file to determine if the logon is correct.

With Windows NT Version 4 installed with Service Pack 3, passwords are no longer sent unencrypted on the network, and the Samba server cannot immediately check them against the /etc/passwd file. To bypass the NT machine's increased security, you have two choices. You can either decrease the level of security on the NT machine or increase the level of security on your Samba server.

7.6.1 Decreasing the Level of Security on Your NT Client

The level of security used for sending encrypted passwords on the network is controlled by the registry. You must be logged in as administrator to modify security levels. To modify the registry, perform the following steps:

1. Run **Registry Editor** (Regedt32.exe).
2. From the HKEY_LOCAL_MACHINE subtree, go to \SYSTEM\CurrentControlSet\Services\Rdr\Parameters.
3. Click **Add Value** on the Edit menu.
4. Add the following:
   ```
   Value Name: EnablePlainTextPassword
   Data Type: REG_DWORD
   Data: 1
   ```
5. Click on **OK** and then quit Registry Editor.
6. Shut down and restart Windows NT.

After the machine reboots, the passwords are sent non-encrypted over the network, and Samba works correctly.

7.6.2 Increasing the Level of Security on the Samba Server

You can also configure Samba to make it aware of password encryption. Since Release 1.9.18, you don't need the Data Encryption Standard library to let your Samba server deal with encrypted passwords. The explanation of the mechanisms involved with encryption can be found in the /usr/local/samba/doc/ENCRYPTION.txt file. To configure your Samba server there are only a few steps to follow.

1. Create a smbpasswd file. This file is used by the Samba server to analyze the encrypted password sent by the Windows NT machine. This file is created from your /etc/passwd file or from your NIS password map, using the `mksmbpasswd.sh` command. This command is located in the source file of your Samba distributions. The default location for this file is /usr/local/samba/private, and it is very important to protect the access to this file since it contains information that grants access to your server. If you don't use NIS, create the smbpasswd file by typing this command:

   ```
   cat /etc/passwd | mksmbpasswd.sh >/usr/local/samba/private/smbpasswd
   ```

   If you use NIS, use this command:

   ```
   ypcat passwd | mksmbpasswd.sh >/usr/local/samba/private/smbpasswd
   ```

2. Modify the smb.conf file to use encrypted passwords. The parameter in the smb.conf file that decides if Samba will use encrypted passwords or not is listed below:

   ```
   encrypt passwords = yes
   ```

3. Restart the Samba daemons.

Your next attempt to access the Samba server will be successful. Though this doesn't sound difficult to do, be aware that each time your UNIX users change their UNIX passwords, they will have to use the `/usr/local/samba/bin/smbpasswd` command to reflect the modification in the smbpasswd file.

7.6.3 Using a Remote Machine to Make the Authentication

Another method you have to handle this password problem is to let someone else do the authentication of the passwords. It can be a trusted NT server or another Samba server. There are two parameters to change in the smb.conf file to perform this operation. Use the following if you are going to let someone do the authentication:

```
security = server
```

This second modification provides the Samba server with the name of the remote machine:

```
password server = itsont00
```

Restart the Samba daemons. Now each time the Samba server receives a request, it will forward the login and password to the remote machine to grant access to the client.

7.6.4 NT to AIX Users Mapping

It may happen that the name of your users on their client stations are not the ones they want to connect with on the Samba server. Samba provides a mechanism that allows the mapping of NT usernames to AIX usernames. For example, if you want users logged on the NT client as admin or administrator to be able to log onto your Samba server as root, you just have a few steps to perform:

1. Edit the smb.conf file and add a parameter that specifies the name and location of the file that contains the correspondence between the NT and AIX users:

   ```
   username map = /usr/local/samba/lib/user.map
   ```

2. Then add a line in the /usr/local/samba/lib/user.map file that will show that users logged as admin or administrator on the NT machine should be logged on the AIX machine using the root user.

   ```
   root = admin, administrator
   ```

3. Restart the Samba daemons

From now on, any users logged onto a NT system with the user admin or administrator can access the Samba server and provides the root password for authentication, the translation between the pair admin/password and root/password will be done automatically by Samba.

7.7 Limitations

During our tests, the ability to browse the Network Neighborhood from a Windows NT client seemed to only work intermittently. There is a file named /usr/local/samba/doc/BROWSING.txt that comes with Samba that suggests browsing has been a problem. Using Windows Explorer however, we are still able to access the server and map a drive by using the standard reference of \\SERVERNAME.

7.8 Troubleshooting

The Samba product seems to be very reliable and there are only a few tips needed to keep your server up and running:

- If you can not access a shared resource, check that the two daemons, nmbd and smbd, are running. Use the command `ps -ef | grep mbd` to check their status. If the daemons need to be restarted, the only method is to issue the `kill` command against the process ID and restart the daemons either from the inetd daemon or with the startup script that starts Samba when the server is originally started.
- Whenever a change is made to the smb.conf file, use the test program provided, /usr/local/samba/bin/testparm, to test that you have not made any syntactic errors in the file format. Incorrect format in the smb.conf file can cause unexpected results once you start the Samba daemons. Another program, /usr/local/samba/bin/testprns, tests for correct definition of printers in the smb.conf file.
- Most diagnostics issued by the server are logged in a specified log file. The log file name is specified at compile time, but may be overridden on the smbd command line. See the smbd man page for more information. The default log files are /usr/local/samba/var/log.smb and /usr/local/samba/var/log.nmb.

  The number and nature of diagnostics available depends on the debug level used by the server. The server can be started with the `-d` option for debug. The valid debug level values are between 0 and 10 with 0 providing only critical error information and 10 providing the most detail. A debug level above 3 is intended for use by developers and generates huge amounts of data that is very cryptic. If you have problems, set the debug level to 3 and peruse the log files.

  Most messages are reasonably self-explanatory. You may need to `grep` the source code for the keyword logged in the log file and inspect the conditions that gave rise to the error you observed in the log file.
- The command `smbclient -L servername` will provide output regarding the shares and services available. Check this output for the existence of the shares or services with which you may be experiencing difficulty.

The Samba Web site and the Samba distribution contains very good documentation. If necessary, refer to the man pages or the How-To pages and Frequently Asked Questions (FAQs) on the Samba Web site, at `http://samba.anu.edu.au`.

Finally, send bug reports, comments, errors and suggestions to samba-bugs@samba.anu.edu.au (Andrew Tridgell).

7.9 Samba and the Year 2000

Samba is year 2000 compliant because the underlying protocol used, SMB, is also year 2000 compliant.

Appendix A. Performance Overview

There are many factors to consider when making decisions about the various products described in this book. The performance figures mentioned here are just indicative. The goal of this appendix is to give you an idea of the relative performance in terms of throughput of these products, compared to a native NT server.

A.1 Performance

When choosing a server, performance can often be deciding factor. In this section we describe how we benchmarked all of the servers:

- AIX Connections
- AS/U
- Novell Network Services
- Samba
- Total Advanced Server
- Windows NT Server 4.0

The protocol used by the products were NetBIOS over TCP/IP except for the Novell Network Services product that was using IPX/SPX.

A.1.1 Benchmarks

We ran two benchmarks on all of the servers:

- A Perl script to test file system performance
- Ziff-Davis Inc. NetBench 5.01

A.1.1.1 Perl Script Benchmark

The Perl script benchmark we used was a very simple single script that ran through the following tests:

- File creation
- Directory listing
- File deletion
- File write (small portions)
- File write (whole file)
- File read (small portions)

- File read (whole file)

The benchmark runs from a single client. A mapped directory from the server to the client is provided as an input parameter. The script runs in three modes. Each mode determines the length of the benchmark:

- Small
- Medium
- Large

The script was run in each of the modes for all of the servers.

The Perl benchmark reports its results as a single figure. The lower the figure, the better the performance of the server being tested.

A.1.1.2 NetBench 5.01

The main test which we used was the Ziff-Davis NetBench 5.01 benchmark program. This is a widely-used benchmark program that tests the performance of file servers. The benchmark does not require any code to be installed on the server and instead relies on a mapped directory from the server to be tested from all of the clients. A controller system collects the data from the clients and creates a Microsoft Excel spreadsheet with the results upon completion of the benchmark. NetBench reports its results as throughput in bytes/second.

NetBench is tool that can be configured in many different ways, allowing a huge number of benchmarks could be generated to test network servers. The NetBench benchmark comes with a default test suite, nbdm_60.tst. This benchmark suite uses the Disk Mix test. The Disk Mix test mirrors the way a number of PC applications use a file server (including Microsoft Office). To find out more about the NetBench benchmark program and download the software, look at their Web page, at `http://www.zdnet.com/zdbop/zdbop2.html`.

To create our benchmark, we modified the standard nbdm_60.tst test suite. Our NetBench benchmark suite runs through four Disk Mix tests:

- Test DM_1 with one client and a workspace of 20 MB.
- Test DM_4 with four clients and a workspace of 20 MB.
- Test DM2_1 with one client and a workspace of 50 MB.
- Test DM2_4 with four clients and a workspace of 50 MB.

The other parameters we set for NetBench were the same for each test:

Ramp Up 30 seconds

Ramp Down	30 seconds
Length	10 minutes
Delay	5 seconds
Think Time	2 seconds
Save Workspace	Yes

A.1.1.3 Clients

For all of the benchmarks, we used four clients. For consistency all of the clients used for testing the servers were identical and had the following specifications:

Operating System	Windows NT 4.0
Processor	Intel Pentium 166 Mhz
Number of processors	1
Memory	64 MB
32-bit File Access	Yes
File Cache Size	0
32-Bit Disk Access	Yes
Network Client	Microsoft Client
Protocol	NetBIOS (TCP/IP)
Network Card	IBM Token-Ring 16 MB

All tests, excluding NNS, used to default Microsoft Client included with Windows NT 4.0. The NetBench failed to run using the Microsoft NetWare client so we installed the Novell IntraNetWare Client for Windows NT.

A.1.1.4 Servers

All of the RS/6000 servers that we tested with the benchmarks had exactly the same specifications:

Operating System	AIX V4.2.1
Processor	PowerPC 604 132 Mhz
SPECint95	4.72
SPECfp95	3.76
Number of Processors	1
Memory	64 MB
Disk Subsystem	2 GB IBM SCSI-II external disk

Network Card	IBM Token-Ring 16 MB

The Windows NT server that was benchmarked had the following specifications:

Operating System	Windows NT 4.0
Processor	Intel Pentium 166 Mhz
SPECint95	4.8 (estimated)
SPECfp95	3.8 (estimated)
Number of Processors	1
Memory	64 MB
Disk Subsystem	2 GB internal IBM IDE disk
Network Card	IBM Token-Ring 16 MB

A.1.2 Results

This section presents the results of the two benchmarks for all the servers. A "-" indicates that a test failed to run or did not complete. All of the benchmarks were run on a production network, not a private network. The tests were all run, however, when there were few users and very little network traffic generated by the users.

7.9.0.1 Perl Script Results

The results from the perl benchmark are shown in Table 5. The smaller numbers represent better results. The results give a rough indication of how the different products perform against each other.

Table 5. Perl Benchmark Results

Server	Small	Medium	Large
AIX Connections	200	400	230
AS/U	100	300	210
NNS	200	400	320
Samba	200	300	170
TAS	252	320	320
Windows NT	100	200	130

A.1.2.1 NetBench Results

The NetBench results show a more accurate picture of the servers' performance. The results, however, are only one iteration of the NetBench benchmark. To get a full picture would require testing the servers with several different combinations of NetBench configurations.

Table 6 shows the total combined throughput for all four tests run on each of the servers in kilobytes per second. The final column shows the average CPU utilization of the server while running the benchmark (this was obtained using `vmstat` on the RS/6000 server).

Table 6. NetBench Total Throughput Results

Server	DM_1	DM_4	DM2_1	DM2_4	CPU Utilization
AIX Connections	107 KB/s	318 KB/s	106 KB/s	326 KB/s	-
AS/U	208 KB/s	499 KB/s	210 KB/s	495 KB/s	50 percent
NNS	160 KB/s	295 KB/s	161 KB/s	291 KB/s	33 percent
SAMBA	304 KB/s	617 KB/s	305 KB/s	649 KB/s	28 percent
TAS	110 KB/s	337 KB/s	113 KB/s	342 KB/s	33 percent
Windows NT	232 KB/s	612 KB/s	233 KB/s	605 KB/s	-

For each test, the maximum throughput of any single client was recorded. Table 7 shows this peak throughput (in kilobytes per second) for a client in all four tests.

Table 7. Peak Throughput of a Client

Server	DM_1	DM_4	DM2_1	DM2_4
AIX Connections	107 KB/s	83 KB/s	106 KB/s	83 KB/s
AS/U	208 KB/s	131 KB/s	210 KB/s	132 KB/s
NNS	160 KB/s	81 KB/s	161 KB/s	82 KB/s
Samba	304 KB/s	161 KB/s	305 KB/s	169 KB/s
TAS	110 KB/s	88 KB/s	113 KB/s	88 KB/s
Windows NT	232 KB/s	166 KB/s	233 KB/s	168 KB/s

For each test, the minimum throughput of any single client was recorded. Table 8 shows this lowest throughput (in kilobytes per second) for a client in all four tests.

Table 8. Minimum Throughput per Client

Server	DM_1	DM_4	DM2_1	DM2_4
AIX Connections	107 KB/s	77 KB/s	106 KB/s	80 KB/s
AS/U	208 KB/s	106 KB/s	210 KB/s	108 KB/s
NNS	160 KB/s	71 KB/s	161 KB/s	66 KB/s
SAMBA	304 KB/s	150 KB/s	305 KB/s	157 KB/s
TAS	110 KB/s	82 KB/s	113 KB/s	84 KB/s
Windows NT	323 KB/s	145 KB/s	232 KB/s	124 KB/s

Appendix B. Comparison Table

This table summarizes the key functionalities or properties of the products described in this book.

Table 9. Comparison of Various Key Points for These Products

	Samba	NNS	AS/U	AIX Conn.	TAS
Turns AIX into a file server	Y	Y	Y	Y	Y
Turns AIX into a file client	Y smbclient	N	Y lmshell	Y	Y
Turns AIX into a print server	Y	Y	Y	Y	Y
Turns AIX into a print client	N	N	N	Y smbprint	Y
Turns AIX into a primary domain controller	N	N	Y	N	N
Turns AIX into a backup domain controller	N	N	Y	N	N
Lets AIX be part of a trust relationship	N	N	Y	N	N
Turns AIX into a WINS server	N	N	Y	N	N
Allows NT user creation	N	N	Y	N	N
Allows NT profile management	N	N	Y	N	N
Allows NT/AIX users mapping	N	Y	Y	Y	Y
Provides NetWare integration	N	Y	N	Limited	Limited
Provides LDAP support	N	Y	N	N	N
Allows NT files replication	N	N	Y	N	N
Send messages	Y	Y	Y	Y	Y
Time synchronization	Y	Y	Y	Y	Y
Long file names support	Y	Y	Limited	Y	Y
IBM support	N	Y	N	Y	Limited

Appendix C. Special Notices

This publication is intended to help system engineers, I/T architects, and consultants understand the various products that can be installed on the AIX operating system to better integrate with Windows NT systems. The information in this publication is not intended as the specification of any programming interfaces that are provided by AIX Connection, TotalNET Advanced Server, Advanced Server for UNIX, Novell Network Services or Samba. See the PUBLICATIONS section of the IBM Programming Announcement for AIX Connections and Novell Network Services 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 pointers in this publication to external Web sites are provided for convenience only and do not in any manner serve as an endorsement of these Web sites.

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.

The following document contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples contain the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

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.

You can reproduce a page in this document as a transparency, if that page has the copyright notice on it. The copyright notice must appear on each page being reproduced.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

AFP	AIX ®
AT ®	IBM ®
OS/2 ®	PowerPC 604 ®
RS/6000	SP

The following terms are trademarks of other companies:

C-bus is a trademark of Corollary, Inc.

Java and HotJava are trademarks of Sun Microsystems, Incorporated.

Microsoft, Windows, Windows NT, and the Windows 95 logo are trademarks or registered trademarks of Microsoft Corporation.

PC Direct is a trademark of Ziff Communications Company and is used by IBM Corporation under license.

Pentium, MMX, ProShare, LANDesk, and ActionMedia are trademarks or registered trademarks of Intel Corporation in the U.S. and other countries.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Other company, product, and service names may be trademarks or service marks of others.

Appendix D. Related Publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

D.1 International Technical Support Organization Publications

For information on ordering these ITSO publications see “How to Get ITSO Redbooks” on page 327.

- *AIX V4.2 and Windows NT 4.0, Side by Side*, SG24-4784
- *AIX Connections for Beginners*, SG24-4588

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
Lotus Redbooks Collection	SBOF-6899	SK2T-8039
Tivoli Redbooks Collection	SBOF-6898	SK2T-8044
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
RS/6000 Redbooks Collection (PDF Format)	SBOF-8700	SK2T-8043
Application Development Redbooks Collection	SBOF-7290	SK2T-8037

D.3 Other Publications

These publications are also relevant as further information sources:

- *Novell Network Services 4.1 for AIX Quick Beginnings*, SC23-4131
- *Introduction to NetWare Directory Services*, SC23-4132
- *Novell Network Services 4.1 for AIX Supervising the Network*, SC23-4140
- *AIX Connections V4: Quick Beginnings*, SC23-1758

- *AIX Connections, Reference Guide*, SC23-1829
- *AIX Connections, Client Guide*, SC23-1762
- *AIX Connections, Administrators Guide*, SC23-1828

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 `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 BookManager BOOKs of redbooks, type the following command:

  ```
  TOOLCAT REDBOOKS
  ```

  To get lists of redbooks, type the following command:

  ```
  TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET ITSOCAT TXT
  ```

  To register for information on workshops, residencies, and redbooks, type the following command:

  ```
  TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ITSOREGI 1998
  ```

  For a list of product area specialists in the ITSO, type the following command:

  ```
  TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ORGCARD PACKAGE
  ```

- **Redbooks Web Site 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	1-800-267-4455
Outside North America	(+45) 48 14 2207 (long distance charge)

- **1-800-IBM-4FAX (United States)** or **(+1) 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 Web Site	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.

List of Abbreviations

AFP	Apple File and Print Protocol
AFS	Andrew File System
AIX	advanced interactive executive
ANSI	American National Standards Institute
AS/U	Advanced Server for UNIX
ATM	asynchronous transfer mode
BDC	backup domain controller
CN	common names
CPU	central processing unit
CSR	Customer Service Request
DAP	Directory Access Protocol
DLPI	data link provider interface
DNS	domain name service
DOS	disk operating system
FAT	file allocation table
FDDI	fiber distributed data interface
HTML	Hypertext Markup Language
iFOR/LS	Information For Operation Retrieval/License System
IBM	International Business Machines Corporation
IPF	Install Package Facility
IPX	Internetwork Packet eXchange
ITSO	International Technical Support Organization
LAN	local area network
LANA	local area network adapter
LDAP	Lightweight Directory Access Protocol
LPP	licensed program products
LPR	line printer
NCP	NetWare Core Protocol
NCPS	Novell Cross-Platform Services
NDS	Novell Directory Services
NFS	network file system
NIS	network information system
NNS	Novell Network Services
NPS	NetWare Protocol Stack
NTFS	NT File System
NUC	NetWare UnixClient
NetBEUI	NetBIOS Extended User Interface
OEM	original equipment manufacturer
PC	personal computer
PDC	primary domain controller
PPA	Physical Point of Attachment
RFC	request for comments
RIP	routing information protocol
RS/6000 SP	IBM RS/6000 Scalable POWERParallel Systems
SAM	Security Accounts Manager
SANDS	Standalone NDS
SAP	Service Advertising Protocol
SAPD	SAP daemon
SCALE	Scalable NDS
SMB	Server Message Block
SMP	symmetric multiprocessor
SNMP	simple network management protocol
SP	Scalable POWERParallel
SPX	Sequenced Packet eXchange
TAS	TotalNET Advanced Server
TCP/IP	Transmission Control Protocol/Internet Protocol
TNAS	TotalNET Administration Suite
VMS	virtual memory system

WINS	Windows Internet Name Service
Windows NT	Windows New Technology

Index

Symbols

A

B

C

O

P

R

S

T

U

V

W

X

Y

ITSO Redbook Evaluation

AIX and Windows NT Solutions for Interoperability
SG24-5102-00

Your feedback is very important to help us maintain the quality of ITSO redbooks. **Please complete this questionnaire and return it using one of the following methods:**

- Use the online evaluation form found at http://www.redbooks.ibm.com
- Fax this form to: USA International Access Code + 1 914 432 8264
- Send your comments in an Internet note to redbook@us.ibm.com

Please rate your overall satisfaction with this book using the scale:
(1 = very good, 2 = good, 3 = average, 4 = poor, 5 = very poor)

Overall Satisfaction _____

Please answer the following questions:

Was this redbook published in time for your needs? Yes___ No___

If no, please explain:

_____

_____

_____

_____

_____

What other redbooks would you like to see published?

_____

_____

_____

Comments/Suggestions: (THANK YOU FOR YOUR FEEDBACK!)

_____

_____

_____

_____

_____

AIX and Windows NT Solutions for Interoperability

SG24-5102-00

SG24-5102-00
Printed in the U.S.A.