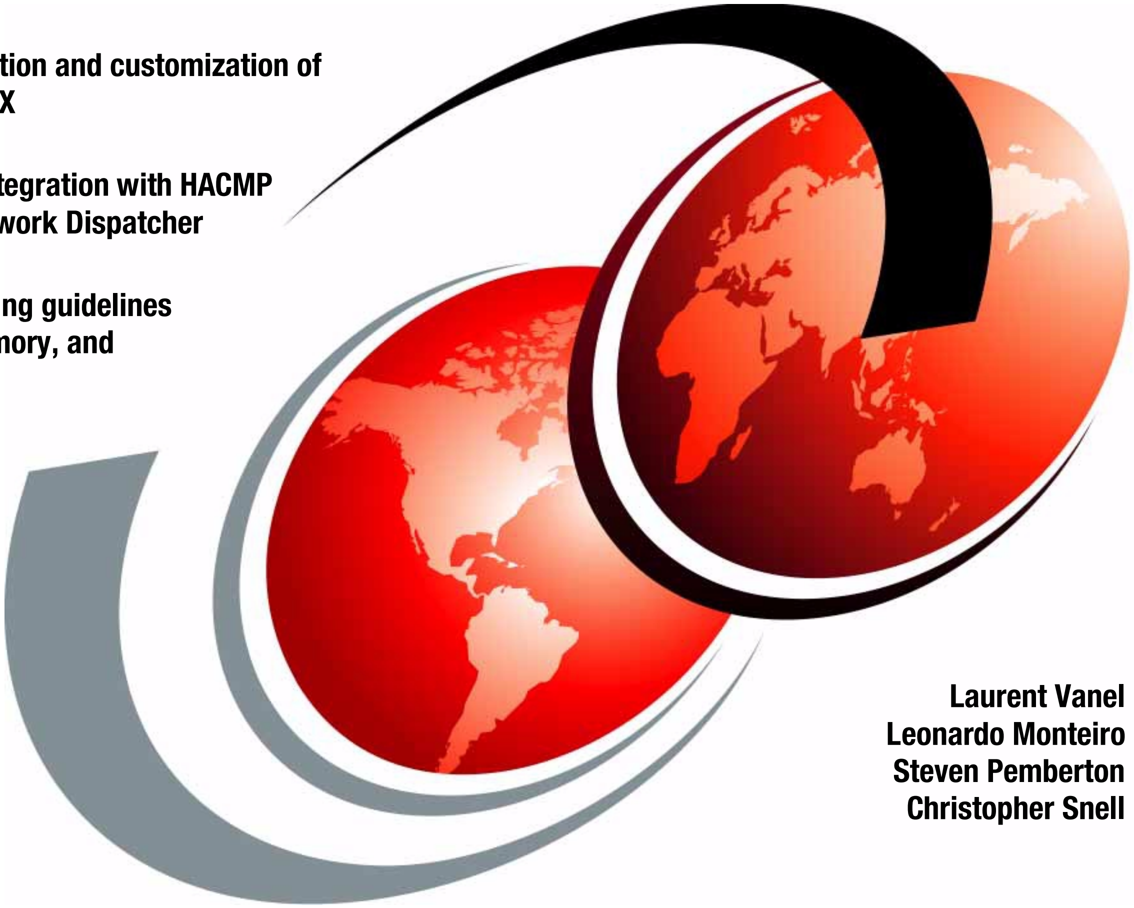
Samba

Installation, Configuration, and Sizing Guide

Easy installation and customization of Samba on AIX

Advanced integration with HACMP and IBM Network Dispatcher

Practical sizing guidelines for CPU, memory, and network



Laurent Vanel
Leonardo Monteiro
Steven Pemberton
Christopher Snell

Redbooks

ibm.com/redbooks

SG24-6004-00

International Technical Support Organization

Samba Installation, Configuration, and Sizing Guide

July 2000

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix B, “Special notices” on page 205.

First Edition (July 2000)

This edition applies to Version 2.0.6 of Samba for use with the AIX Operating System.

Comments may be addressed to:
IBM Corporation, International Technical Support Organization
Dept. JN9B Building 003 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

Samba is the very popular freeware that turns your AIX machine into a resources server for your PC clients. This book explains how to install and set up a Samba server, how to declare file and printer shares, and how to choose the best security model that fits your needs.

But it won’t cover all the features of Samba in detail. Many books exist that do this already. This book focuses on AIX-specific advantages for Samba, obtaining a highly-available Samba server with HACMP, a powerful Samba server with IBM eNetwork Dispatcher, or putting Samba under the control of the AIX System Resources Controller.

This book also describes how to customize your PC clients running Windows 95, Windows 98, Windows NT, Windows 2000, or OS/2 to access the SambaServer.

Finally, in this book, you will find some sizing guidelines for a Samba server, which server to choose, and which configuration, based on the number of PC clients and activity in your environment, to choose.

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.

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 when the first RS/6000s were announced. Since then, he has provided AIX support to both field engineers and customers.

Leonardo Monteiro is a Solution Architect in Brazil. He has five years of experience in AIX and Windows. He has worked on AIX and Windows NT support teams. He holds a degree in Mechanical Engineering from Federal Fluminense University, and his areas of expertise include AIX and SP Administration, Notes, and Tivoli Storage Manager.

Steven Pemberton is a System Administrator in Australia. He has five years of experience in UNIX and Windows Administration. He has worked at Utili-Mode for four years and leads their Technical Services AIX team. Steven is currently president of the Victorian group of the System Administrator’s Guild of Australia (SAGE-AU). His areas of expertise include AIX and SP administration, Tivoli Storage Manager, and HACMP administration.

Christopher Snell is a Software Engineer in the USA. He has six years of experience in the System and Network Administration field and has worked at IBM for one year. He holds a bachelor of science degree in Computer Science from Johns Hopkins University. His areas of expertise include Windows Networking.

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

The entire Samba team and Samba user community, especially Peter Samuelson and Andrew Tridgell for technical advice during the production of this Redbook

Lee Terrell
IBM Austin

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 “IBM Redbooks review” on page 219 to the fax number shown on the form.
- Use the online evaluation form found at `http://www.redbooks.ibm.com/`
- Send your comments in an Internet note to `redbook@us.ibm.com`

Chapter 1. Introduction to Samba

Samba is a suite of programs that work together to allow clients to access server file systems and printers via the Server Message Block (SMB) and Common Internet File System (CIFS) protocols.

Although it was initially written for UNIX, Samba also runs on S/390, NetWare, OS/2, MPE/ix, and VMS. Samba is available free-of-charge according to the rules of the GNU Public License.

In this Redbook, we describe running Samba 2.0.6 on an RS/6000 with AIX 4.3.3.

1.1 Function overview

Samba implements the SMB/CIFS protocols that enable clients and servers to exchange messages and data. Samba enables UNIX systems to act as file and print servers for PC client systems. Although Samba is primarily used to provide Windows-like file and print services under UNIX, it also includes UNIX SMB client utilities.

Windows 95/98, Windows NT, Windows 2000, and OS/2 Warp clients do not need any extra software to access a Samba server. These operating systems all support NetBIOS over TCP/IP (NBT), which is all that is needed to access a Samba server.

Samba provides the following features:

- Windows-like SMB file and print server.
- Acts as a Primary Domain Controller.
- Participation in an existing domain (passthrough authentication).
- Browsing support: Samba can be the domain or local master browser.
- NetBIOS name resolution service (similar to Microsoft WINS).
- A Web-based configuration tool (SWAT).
- Command line SMB client (similar to FTP).
- A tar extension for backing up client PCs.

1.2 SMB networking overview

Before installing Samba, it is important to have an understanding of Windows networking concepts. Windows-style SMB file and print services differ from UNIX file and print services in many ways.

In 1984, IBM and Sytec coauthored a simple API called Network Basic Input/Output System (NetBIOS). This was extended in 1985 and named NetBIOS Extended User Interface (NetBEUI). NetBEUI was limited to small LANs since it is a non-routable protocol.

To add network routing support, NetBIOS was later hosted on top of IPX, DECNet, and TCP/IP. As TCP/IP gained popularity, NetBIOS over TCP/IP (NBT) has become the most common implementation. Samba only implements NetBIOS over TCP/IP.

NetBIOS over TCP/IP uses the threeTCP/IP ports listed in Table 1.

Table 1. TCP/IP ports used by NetBIOS over TCP/IP

Port 137	**Name service** Provides NetBIOS browsing information and name resolution.
Port 138	**Datagram service** This service is typically not used.
Port 139	**Session service** Provides file and print shares.

Meanwhile, Microsoft developed the Server Message Block (SMB) protocol. This is a higher level protocol that resides on top of NetBIOS over TCP/IP. SMB offers service announcement (browsing), name resolution (WINS), client-side file caching (oplocks), centralized authentication (a Domain), and many other features.

NetBIOS name resolution varies depending on the type of node and configuration of the client. In its most basic form, NetBIOS clients announce their existence and any services provided across the local network. Other NetBIOS clients cache this information to produce a map of the available network services, thus creating the browse list.

Microsoft's NetBIOS name server is called the Windows Internet Name Service (WINS). Samba can function as a NetBIOS name server but cannot replicate data with Microsoft WINS servers.

The SMB protocol defines two models of security. In the original model, share level security, the client need only provide a password to access a share. A username is not required in share level security. Once a client has access to a share, he or she can access any files contained within that share. The more recent model, user level security, requires the client to provide a username and password to access a share. Additionally, user level security can protect individual files within a share.

A Domain is a collection of computers whose security information is centrally managed by a Domain Controller. There can only be one Primary Domain Controller in any given Domain, although there may be multiple Backup Domain Controllers. In a Workgroup, each client maintains their own security information. Generally, a workgroup is restricted to a single subnet. Since Version 2.0, Samba can function as a Primary Domain Controller.

Recently, Microsoft has enhanced and renamed the SMB protocol to the Common Internet File System (CIFS). The CIFS 1.0 protocol specification has been submitted to the Internet Engineering Task Force (IETF).

1.3 Obtaining Samba

Samba is generally distributed as source code, although several options exist to obtain precompiled binary packages for AIX and other types of UNIX. You must compile the source files once you have retrieved them.

Be aware that the precompiled binaries may not be the latest version, and you give up the option to define custom settings in the makefile that apply to your environment. Another advantage of compiling from source is the added confidence that the program has not been modified by a malicious third party.

Samba is available from the sources described in the following sections.

1.3.1 HTTP

The definitive source for the code, documentation, license information, and patches is available on the Web at the following URL:

```
http://www.samba.org
```

The most recent version is downloadable as:

```
http://us1.samba.org/samba/ftp/samba-latest.tar.gz
```

Samba can also be obtained in AIX installp format. This version is the easiest to install since the installation process makes the necessary modifications to /etc/services and /etc/inetd.conf during the installation. It can be found at the following address:

```
http://www-frec.bull.com/docs/download.htm
```

The Samba installp package installs into a non-standard directory. The Samba binary files are located in /usr/local/bin. Configuration files are located in /usr/local/lib, and log files are located in /var/samba

Precompiled binaries are also available for some other UNIX types and can be downloaded from the following address:

```
http://us1.samba.org/samba/ftp/Binary_Packages/
```

1.3.2 FTP

The definitive source for the code, documentation, license information, and patches is also available via anonymous FTP at the following URL:

```
ftp://ftp.samba.org/pub/samba
```

The most recent version is downloadable as:

```
ftp://ftp.samba.org/pub/samba/samba-latest.tar.gz
```

1.3.3 CVS

The most recent developmental versions of Samba are, generally, only available via Concurrent Version System (CVS). CVS extends the Revision Control System (RCS) to allow remote, concurrent editing of sources by several users. RCS is a common source code versioning system. You can use CVS to get anonymous read-only access to the Samba source code.

> **Note**
>
> You should only need to obtain the latest development versions if you need a specific feature or intend to contribute patches back to the project. You should *never* run the development code in a production environment!

1.3.3.1 Configuring CVS on AIX

Since neither CVS nor RCS are provided with AIX, if you intend to retrieve Samba with this method, you will need to install these products. CVS and RCS are both distributed under the GNU Public license and are freely available on the Internet.

You can download source for CVS from Cyclic Software at the following URL:

```
http://www.cyclic.com
```

You can download source for RCS from the GNU project:

```
ftp://ftp.gnu.org/gnu/rcs
```

Configure RCS and CVS as per their respective documentation.

1.3.3.2 Downloading Samba via CVS

Once CVS is installed and configured, you can use it to download Samba with the following command:

```
cvs -d :pserver:cvs@cvs.samba.org:/cvsroot login
```

When it asks you for a password, type `cvs`.

If you are using a firewall, you may need to talk to your Network Administrator to gain access through the firewall.

Next, run the command:

```
cvs -d :pserver:cvs@cvs.samba.org:/cvsroot co samba
```

This will create a directory called samba/ containing the latest source code.

Whenever you want to merge in the latest code changes, use the following command from within the samba/ directory:

```
cvs update -d -P
```

If you instead want the latest source code for the TNG tree run command:

```
cvs -d :pserver:cvs@cvs.samba.org:/cvsroot co -r SAMBA_TNG samba
```

1.3.4 Other sources

Several commercial books about Samba now exist, and, often, these provide a copy of the Samba source code on CDROM. Be aware that Samba is a rapidly-evolving product, and these CDROMs may not contain the latest version.

1.4 Samba support

The primary means of support for Samba is the Internet. Various Web sites, mailing lists, and newsgroups provide information to assist administrators in solving problems themselves. Increasingly, however, commercial support is available for those who require it.

1.4.1 Self support

The full set of Samba documentation and FAQs is installed with the product under the Samba directory structure. The SWAT configuration tool has links to most of this documentation. These should be your first reference in case of difficulty.

The Samba Web site and mailing lists are a good source for support and how-to information. There are also several newsgroups that contain Samba-related discussions, but they are not restricted to Samba.

If no answer can be found in the following forums, one can send bug reports and problems via e-mail to `samba-bugs@samba.org`.

1.4.1.1 Web site

The most recent documentation and FAQs are available online from:

`http://us1.samba.org/samba/docs/`

1.4.1.2 Mailing lists

There are several mailing lists catering to both user and developer discussions. Note that some of these mailing lists have fairly high amounts of traffic, and you may wish to subscribe to the *digest* version.

• samba:	The Samba SMB file server
• samba digest:	Digest form of Samba list
• samba-announce:	Samba Announcements
• samba-ntdom:	NT domain controller support
• samba-cvs:	Samba CVS commit messages
• samba-docs:	Discussion about Samba documentation
• samba-binaries:	Developer discussions about binary distributions
• samba-technical:	Developer discussions about Samba internals

You can subscribe to the mailing lists by sending e-mail to `listproc@samba.org`. Leave the subject line of the e-mail blank and enter the following text in the body of the e-mail:

```
subscribe <Mailing List Name> <Your Name>
```

Substitute the mailing list name for `<Mailing List Name>` and your name for `<Your Name>`.

1.4.1.3 News groups

Although no one newsgroup is dedicated to Samba discussion, a couple of newsgroups do cover material relevant to Samba:

- `news://comp.protocols.smb`

- `news://mailing.unix.samba`

1.4.2 Commercial support

The Samba Web site lists over 150 companies around the world that offer to support Samba on a commercial basis.

You should review the list at the following URL and make a decision based on your in-house abilities, resource issues, and management expectations.

`http://us1.samba.org/samba/support/`

We have generally found Samba to be highly-reliable and requiring little support once installed.

Chapter 2. Installing Samba on AIX

This chapter describes the two most common methods for installing Samba on AIX and how to ensure that either method results in a successful installation. First, we will discuss the use of a precompiled binary package, and then we will move on to the do-it-yourself approach with the source code.

2.1 Installation with installp

In this section, we discuss how to install the Samba server using the installp binary for Samba. You will need to download the Samba installp freeware code and install the code. Perform the following steps:

1. Download Samba from the following Web site:

   `http://www-frec.bull.com/docs/download.htm`

2. Type `chmod 755 SAMBA-2.0.6.0.exe`
3. Type `./SAMBA-2.0.6.0.exe`
4. Type `inutoc`
5. Type `smitty install`

The installation process modifies /etc/services and /etc/inetd.conf. The /etc/inetd.conf file now includes the smbd, nmbd, and SWAT entries, although you will have to uncomment the entry for SWAT.

After the installation, the following directory structure exists:

- /usr/local/bin - Samba binaries
- /usr/local/lib - smb.conf configuration file and Samba directory structure
- /usr/local/man - Samba man pages
- /var/samba - Logs and miscellaneous files

If your machine is correctly installed and configured, it will now be able to act as a SMB server and provide information about the shares available. The installp installation starts both smbd and nmbd and puts a default smb.conf configuration file in /usr/local/lib. Use the `smbclient` command to test the installation:

```
/usr/local/bin/smbclient -L yourhostname
```

If this command shows a list of the resources configured in smb.conf, you have a properly-running Samba server. You should now be able to access the shared resources from your clients.

To enable and start SWAT (the Web-based Samba administration interface) perform the following steps:

1. Uncomment the SWAT entry in /etc/inetd.conf
2. Type `refresh -s inetd`

Note that SWAT modifies the Samba configuration file, which is stored in /usr/local/lib/smb.conf. It will rearrange any entries and delete all include= and copy= options and comments that may be in the file. If you wish to preserve any or all of these items, you must either back up your file or not use SWAT.

Now, using a Web browser, go to the following Web site:

```
http://yourhostname:901
```

and log in as root using the ordinary AIX root password.

Note

Using SWAT in this way will send your root password in clear, unencrypted text across the network. This is not an advisable procedure. There are ways around this, but they are not covered here.

You can now continue to Chapter 3, “Basic configuration” on page 15.

2.2 Installing from source code

In this section, we discuss how to install Samba by downloading the source code from the Samba site, compiling the code, and then installing the Samba daemons. The specific configuration steps will be detailed in the next section. You will need to know how to download a file from the Internet, uncompress and extract a file using the `gzip` and `tar` commands, and compile the source using your favorite C compiler to create the binaries necessary to run Samba.

If you have downloaded the precompiled binaries, go directly to Chapter 3, “Basic configuration” on page 15.

2.2.1 Downloading and installing Samba code

The first step in the installation is to download the Samba distribution to your system using one of the methods mentioned in Section 1.3, “Obtaining Samba” on page 3. 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.

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 must also have a C compiler installed.

After extracting the distribution file using the `tar` command, a directory, named samba-2.0.6, is created. At this point, we highly recommend that you read all of the documentation that comes with the distribution before proceeding. The documentation can be found in the main directory and in the docs/ subdirectory.

1. There will be a subdirectory, named source, in which the source files reside; `cd` into this directory. Type `./configure` at the command line to automatically generate a makefile for your particular platform. If you type `./configure --help`, you will be given a list of options that can be used to customize Samba for your environment.

   The `configure` command should finish with statements similar to the following:

   ```
   checking configure summary
   configure OK
   updating cache ./config.cache
   creating ./config.status
   creating include/stamp-h
   creating Makefile
   creating include/config.h
   $
   ```

2. Now, type `make` to create the binaries.

   If you are compiling with the IBM Visual Age C compiler and receive the warning message:

   ```
   1500-030: (I) INFORMATION: <filename>: Additional optimization may be
   attained by recompiling and specifying MAXMEM option with a value
   greater than 2048."
   ```

   you should change the CFLAGS option in the Makefile from CFLAGS=-O to CFLAGS=-O2 -qmaxmem=16384 and recompile.

3. After the `make` command runs successfully, type `make install` to install the binaries and man pages. By default, the Samba distribution is installed in /usr/local/samba. If necessary, this may be changed at compile time by giving the --with-prefixdir= option to configure.

2.2.2 Configuring the Samba daemons

At this point, Samba is installed on your system but needs to be configured prior to use. Let us now see how to configure the daemons that are the base of the Samba product: smbd, nmbd, and SWAT.

The smbd process provides LAN Manager-like services to clients using the SMB protocol. The nmbd process provides NetBIOS name server support to clients. The SWAT process is a self-contained Web server for administration of the Samba server. 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, the appropriate entries must be made manually in the /etc/services and /etc/inetd.conf files.

Ensure that the default ports for Samba are not used by any other program. The default ports for nmbd and smbd are 137 and 139. The default AIX install should already have appropriate entries in the /etc/services file for these ports. The default port for SWAT is generally 901, but any available port lower than 1024 can be used. In case the entries are not in /etc/services, lines similar to the following should be added:

```
netbios-ns 137/udp
netbios-ssn 139/tcp
swat 901/tcp
```

Now, if you wish to use `inetd` to start the Samba daemons, enter suitable lines in the file /etc/inetd.conf, such as the following:

```
netbios-ssn stream tcp nowait root /usr/local/samba/bin/smbd smbd
netbios-ns dgram udp wait root /usr/local/samba/bin/nmbd nmbd
swat stream tcp nowait.400 root /usr/local/samba/bin/swat swat
```

After editing the files, type `refresh -s inetd`.

Starting Samba using a script will cause the server to always be available for client requests. Therefore, starting a client connection may be slightly 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 reason, one of these daemons dies, inetd would restart it automatically at the next request from a client.

If you wish to test your installation without worrying about writing a configuration file, you can use the example that comes with the source distribution. Copy the smb.conf.default file in the examples/ directory of the source tree to /usr/local/samba/lib/smb.conf. Use the `smbclient` command to test the installation:

```
/usr/local/samba/bin/smbclient -L yourhostname
```

If this command shows a list of resources configured in smb.conf, you have a properly-running Samba server. You should now be able to access the shared resources from your clients.

Chapter 3. Basic configuration

Now that we have successfully installed Samba, we can move on to some basic configuration. This chapter will introduce you to the Samba configuration file, smb.conf. We will talk about the format of the file so you can edit it by hand, how to use SWAT to edit the file, and some of the basic, necessary parameters.

3.1 Format of the configuration file

The smb.conf file is the sole configuration file for all of Samba. It is divided into sections that contain parameters. Together, they define specific services, or shares, to be offered to the clients. The file itself is line-based, that is, each newline-terminated line represents either a comment, a section name, or a parameter.

Each section begins with the name of the section in square brackets and continues until the next section begins. The parameters for a section have the syntax name = value. The section and parameter names are not case-sensitive. Lines beginning with a semicolon (';') or a hash ('#') character are ignored, as are lines containing only whitespace. Any line ending in a '\' is continued on the next line in the customary UNIX fashion.

3.1.1 Sections

Each section in the configuration file (except for the [global] section) describes a shared resource, known as a *share*. The section name is the name of the shared resource, and the parameters within the section define the share’s attributes.

Sections are either filespace services (used by the client as an extension of their native file systems) or printable services (used by the client to access print services on the host running the server).

In the smb.conf file, there are three special sections, [global], [homes], and [printers]. Parameters in the [global] section apply to the server as a whole or are defaults for sections that do not specifically define certain items. 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. If a section, called [printers], is included in the configuration file, services connecting clients to the printers on the UNIX machine can be created “on the fly” by the server.

3.1.2 Parameters

Parameters define the specific attributes of sections. Some parameters are specific to the [global] section. Some parameters are usable in all sections. All others are permissible only in normal sections. All of the available parameters are listed and explained in the smb.conf man page.

There are two main types of parameters: Global and network service. The global parameters control the overall behavior of the Samba server and will usually appear only once in the smb.conf configuration file. Network service parameters configure the behavior of specific services, such as shared disks or printers, and will be set on a per-share basis.

The smb.conf file can also take substitutions for some regularly used strings. The most commonly used ones are listed here. These variables are case-sensitive.

%S	Name of the current service
%P	Root directory of the current service
%u	User name of the current service
%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	Home directory of the user given by %u
%v	Samba version
%h	Hostname on which Samba is running
%m	NetBIOS name of the client machine
%L	NetBIOS name of the server
%M	Internet name of the client machine
%I	IP address of the client machine
%T	Current date and time

3.2 Using SWAT

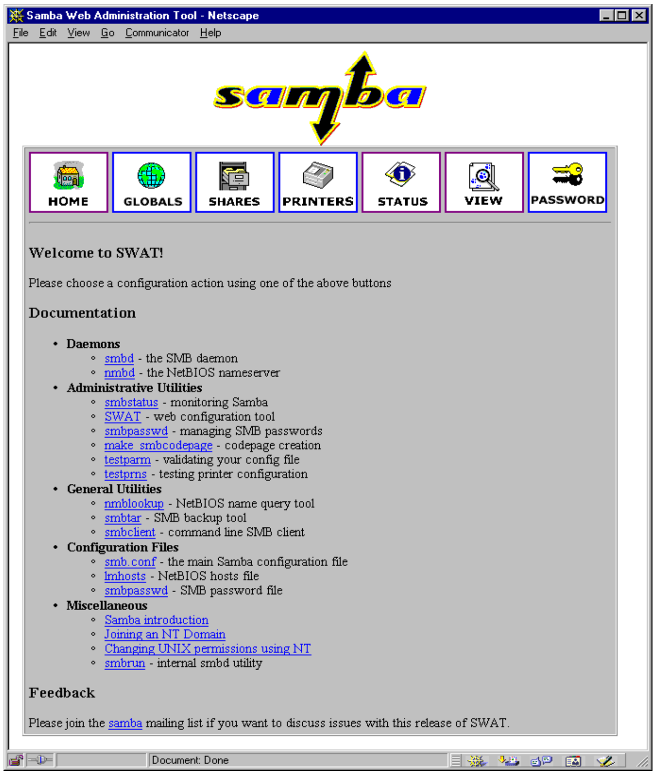
The Samba Web Administration Tool (SWAT) is a common way to set up and maintain the smb.conf configuration file. It presents a nice, simple graphical interface using your favorite Web browser. All of the pages have a similar look and feel; so, it is very easy to learn to use SWAT.

SWAT itself is a small Web server and CGI scripting application designed to run from inetd, which provides access to the smb.conf configuration file. Authorized users can configure the smb.conf file via a Web interface. SWAT also has links to help for each option on every page.

If you set up and configured everything without errors in Chapter 2, “Installing Samba on AIX” on page 9, you are ready to use SWAT. To start SWAT, point your favorite Web browser to the Internet address of your Samba server on port 901. You will be asked to authenticate; so, enter a username and the password of a user defined on your server. You can access SWAT with any AIX user, but you can only make changes when logged in as the root user.

Remember, when you are logging on to SWAT from a remote machine, you are sending passwords in plain text. This can be a security issue; so, it is recommended that you do SWAT administration locally on the server.

If you make any changes to the smb.conf file, the Samba server will reread the file and pick up the changes every 60 seconds. If you cannot wait that long, you can send a HUP signal to the smbd and nmbd daemons to force them to honor the changes. The SWAT opening page is shown in Figure 1. where you will see that there are seven categories available: Home, Globals, Shares, Printers, Status, View, and Passwords.



Welcome to SWAT!

Please choose a configuration action using one of the above buttons

Documentation

- **Daemons**
  - smbd - the SMB daemon
  - nmbd - the NetBIOS nameserver
- **Administrative Utilities**
  - smbstatus - monitoring Samba
  - SWAT - web configuration tool
  - smbpasswd - managing SMB passwords
  - make_smbcodepage - codepage creation
  - testparm - validating your config file
  - testprns - testing printer configuration
- **General Utilities**
  - nmblookup - NetBIOS name query tool
  - smbtar - SMB backup tool
  - smbclient - command line SMB client
- **Configuration Files**
  - smb.conf - the main Samba configuration file
  - lmhosts - NetBIOS hosts file
  - smbpasswd - SMB password file
- **Miscellaneous**
  - Samba introduction
  - Joining an NT Domain
  - Changing UNIX permissions using NT
  - smbrun - internal smbd utility

Feedback

Please join the samba mailing list if you want to discuss issues with this release of SWAT.

Figure 1. SWAT start page

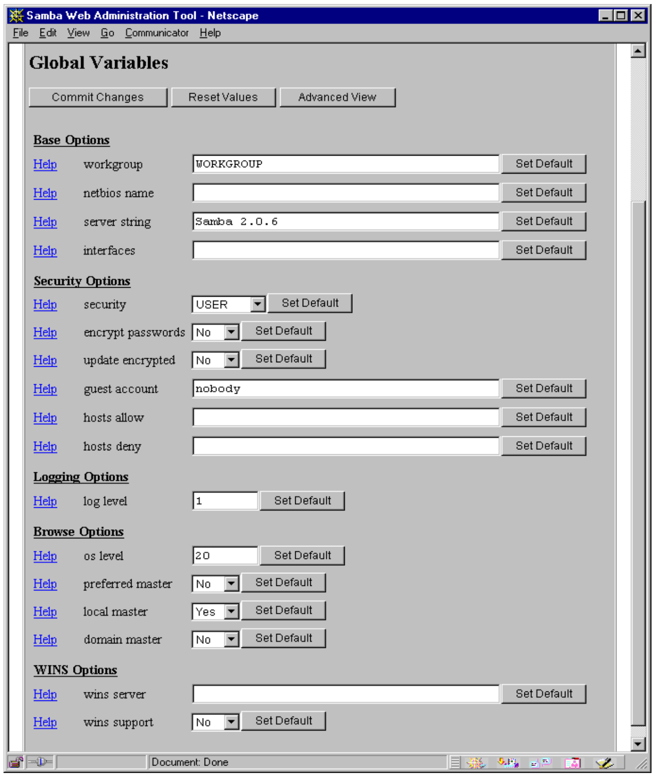
In the following sections, we will briefly describe each of the sections available in SWAT.

3.2.1 Home

The Home page is what is shown in Figure 1 on page 17 and is the same as the start page. From here, you can go to any other section. Also, this page contains links to much of the documentation that comes with Samba.

3.2.2 Globals

When you click the Globals icon in the main SWAT window, you will see a window similar to that shown in Figure 2.



Base Options

Help	workgroup	WORKGROUP
Help	netbios name	
Help	server string	Samba 2.0.6
Help	interfaces	

Security Options

Help	security	USER
Help	encrypt passwords	No
Help	update encrypted	No
Help	guest account	nobody
Help	hosts allow	
Help	hosts deny	

Logging Options

Help	log level	1

Browse Options

Help	os level	20
Help	preferred master	No
Help	local master	Yes
Help	domain master	No

WINS Options

Help	wins server	
Help	wins support	No

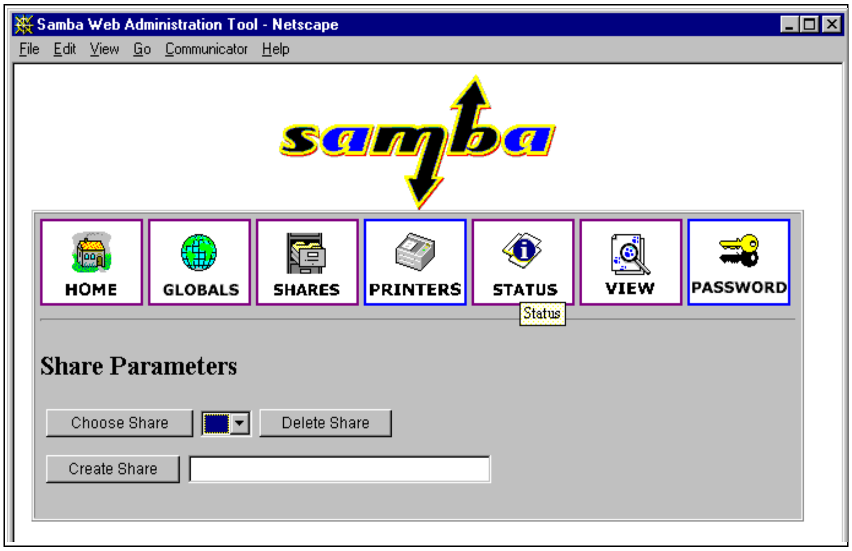
Figure 2. Global section in SWAT

In this window, you can modify global parameters for the Samba server. By default, you will see the Basic View, which only shows you some basic parameters. This is all you really need to get started.

If you want to see all of the available options, click the **Advanced View** button. To return from the Advanced View to the Basic View, click **Basic View**. After you make your changes, you can save them by clicking **Commit Changes**.

3.2.3 Shares

When you click the Shares icon on any SWAT Web page, you will see the screen shown in Figure 3.

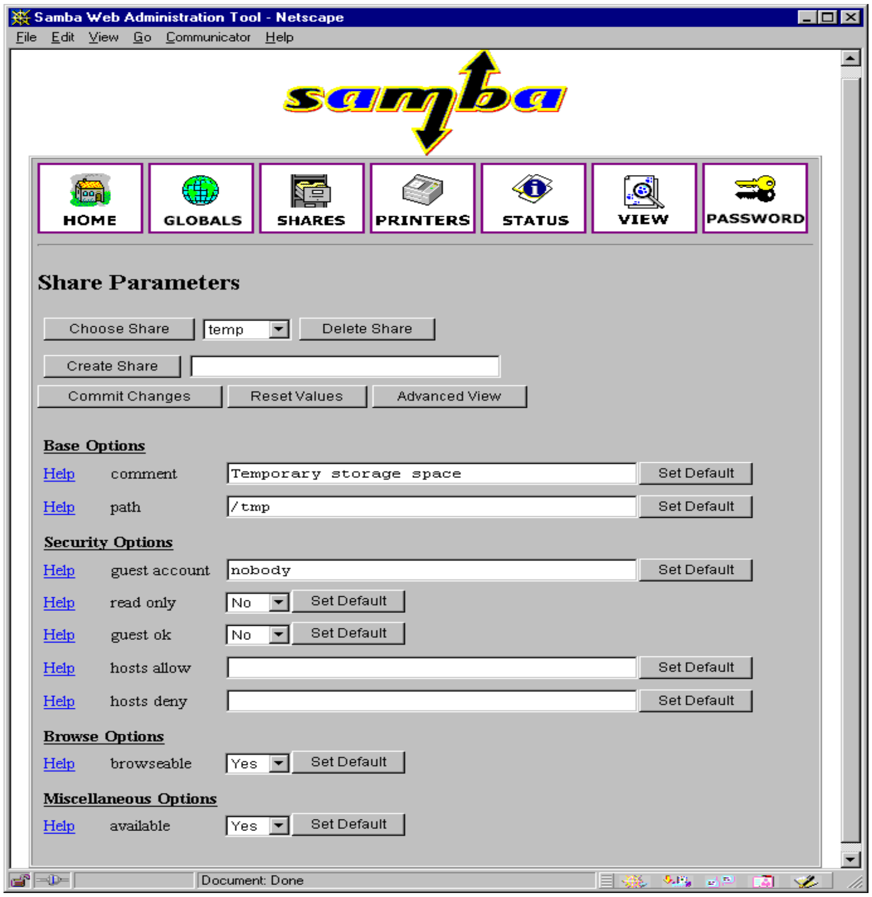


Share Parameters

Figure 3. Shares section in SWAT

Here, you can view a defined share, delete a share, or create a new share.

To view a share, select the share from the drop-down menu and click the **Choose Share** button. You will see a screen similar to that shown in Figure 4 on page 20.



Share Parameters

Choose Share: temp

Base Options

- Help comment: Temporary storage space
- Help path: /tmp

Security Options

- Help guest account: nobody
- Help read only: No
- Help guest ok: No
- Help hosts allow:
- Help hosts deny:

Browse Options

- Help browseable: Yes

Miscellaneous Options

- Help available: Yes

Figure 4. Share Parameters

This will show you a Basic View with only the basic options. If you want to see all available parameters, click **Advanced View**. In this view, you can also make changes, and you can save them by clicking the Commit Changes button.

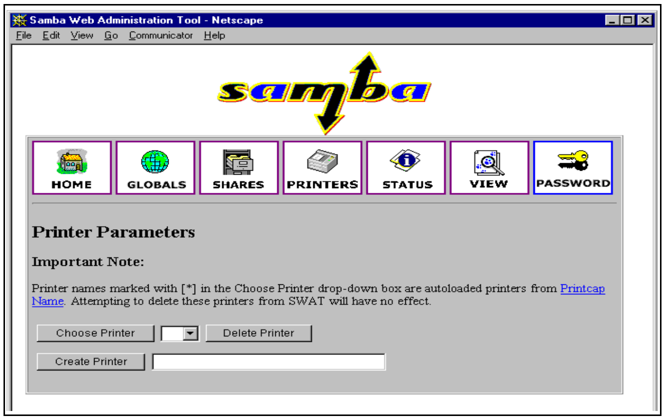
To delete an existing share, you must first select the share, and then click on **Delete Share**. Be careful; the share is deleted immediately and without any further warning.

To create a new share, the directory that will be shared must exist on the server. If it does not, use the `mkdir` command to create it.

Type a name for the share you want to create, and click the **Create Share** button (see Figure 3 on page 19). Now, you will see a screen similar to the shown in Figure 4 on page 20 again. Edit the new share as you would any other share. To save the new share, click **Commit Changes** when you are done.

3.2.4 Printers

In the printers section, you can view, modify, add, or delete printers. The operations for handling printers are the same as for handling shares. You can access printer settings by clicking the Printers icon on any of the SWAT Web pages. You will see a screen similar to that shown in Figure 5.



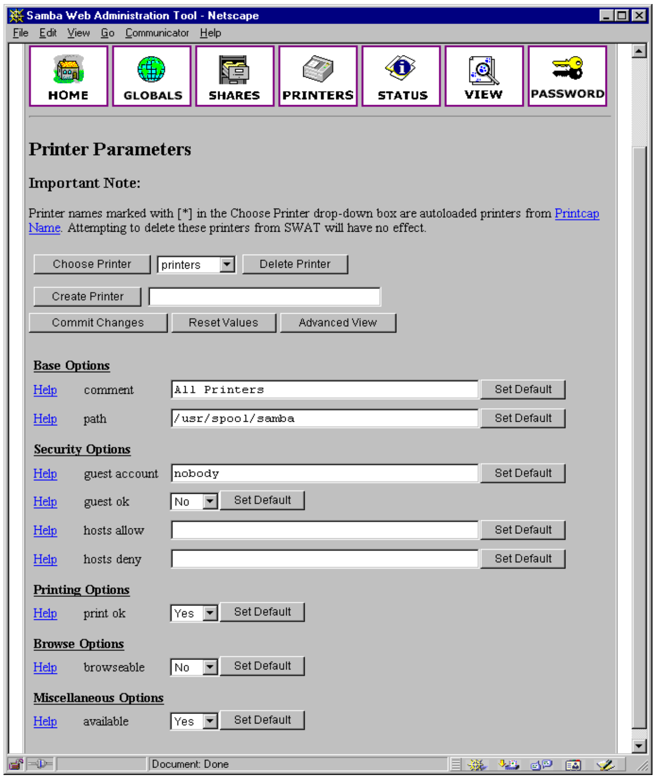
Printer Parameters

Important Note:

Printer names marked with [*] in the Choose Printer drop-down box are autoloaded printers from Printcap Name. Attempting to delete these printers from SWAT will have no effect.

Figure 5. Printer section in SWAT

If you wish to see or change the settings for a specific printer, select the printer from the drop-down menu. After selecting the printer, click the **Choose Printer** button to view the printer's properties, and you will see a screen similar to that shown in Figure 6 on page 22.



Printer Parameters

Important Note:

Printer names marked with [*] in the Choose Printer drop-down box are autoloaded printers from Printcap Name. Attempting to delete these printers from SWAT will have no effect.

Choose Printer: printers

Base Options

Help	comment	All Printers
Help	path	/usr/spool/samba

Security Options

Help	guest account	nobody
Help	guest ok	No
Help	hosts allow	
Help	hosts deny	

Printing Options

Help	print ok	Yes

Browse Options

Help	browseable	No

Miscellaneous Options

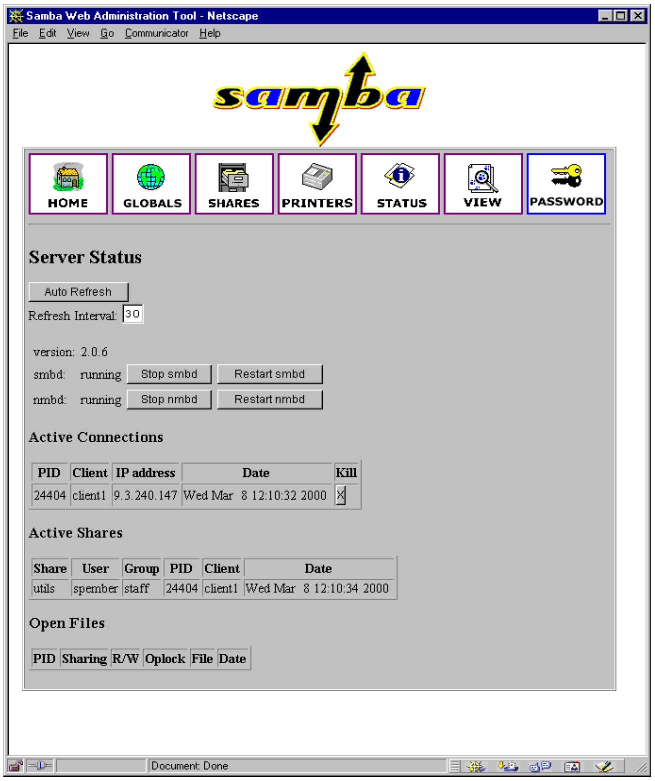
Help	available	Yes

Figure 6. Printer Parameters

In this window, you can also modify printer properties. When you are done, save the settings by clicking the **Commit Changes** button.

3.2.5 Status

In this section, you can check the status of the Samba server. Here, you can view all of the current connections and open files. You can also start or restart the Samba server. The page is shown in Figure 7 on page 23.



Server Status

Refresh Interval: 30

version: 2.0.6

smbd: running

nmbd: running

Active Connections

PID	Client	IP address	Date	Kill
24404	client1	9.3.240.147	Wed Mar 8 12:10:32 2000	X

Active Shares

Share	User	Group	PID	Client	Date
utils	spember	staff	24404	client1	Wed Mar 8 12:10:34 2000

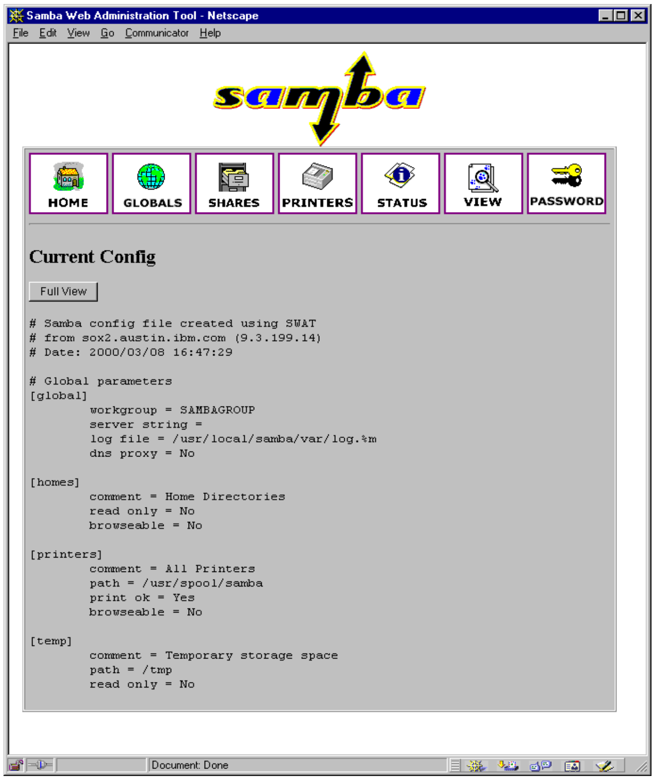
Open Files

PID	Sharing	R/W	Oplock	File	Date

Figure 7. Status section in SWAT

3.2.6 View

In this section, you can see the current smb.conf configuration file. See Figure 8 on page 24 for an example of this page. This will only show the parameters that have been changed from the defaults. You can view detailed options by clicking the Full View button.


Samba Web Administration Tool - Netscape
File Edit View Go Communicator Help
samba
HOME
GLOBALS
SHARES
PRINTERS
STATUS
VIEW
PASSWORD
Full View
Document: Done

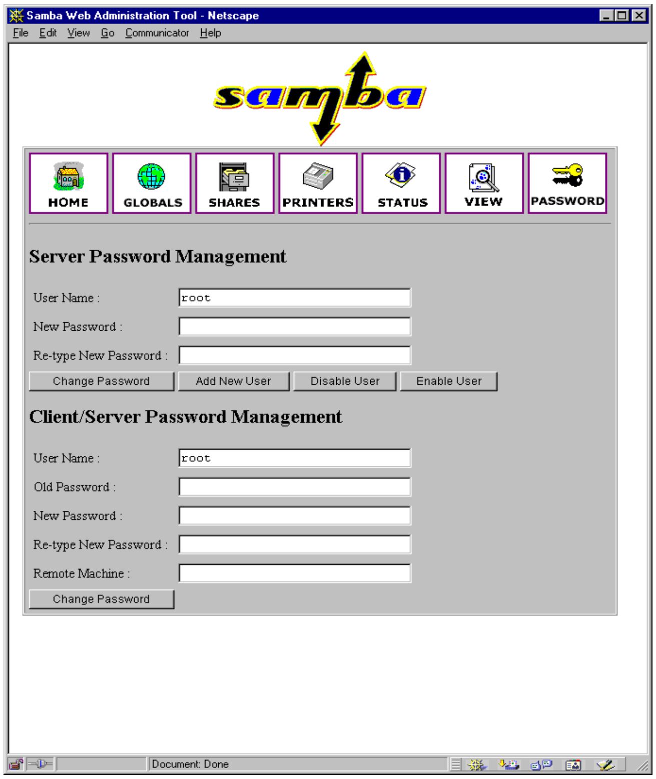
Current Config

```
# Samba config file created using SWAT
# from sox2.austin.ibm.com (9.3.199.14)
# Date: 2000/03/08 16:47:29

# Global parameters
[global]
        workgroup = SAMBAGROUP
        server string =
        log file = /usr/local/samba/var/log.%m
        dns proxy = No

[homes]
        comment = Home Directories
        read only = No
        browseable = No

[printers]
        comment = All Printers
        path = /usr/spool/samba
        print ok = Yes
        browseable = No

[temp]
        comment = Temporary storage space
        path = /tmp
        read only = No
```

Figure 8. View section of SWAT

3.2.7 Password

In this section, you can manage the passwords for all of your Samba users as shown in Figure 9 on page 25.



Server Password Management

User Name : root

New Password :

Re-type New Password :

Client/Server Password Management

User Name : root

Old Password :

New Password :

Re-type New Password :

Remote Machine :

Figure 9. Password section of SWAT

And that is all there is to SWAT. A nice, simple interface to guide you on your way.

3.3 Configuring Samba

Now that we have discussed the ways to edit the smb.conf file, it is time to start talking about the actual parameters. In this section, we will explain how to configure Samba so it can participate as a file and print server in an existing Windows network or be a stand-alone file and print server for Windows clients. We will explain only the most basic parameters. If you need more information, look at the manual page for the smb.conf file or at the Web site for the Samba project:

`http://www.samba.org`

First, let us take a look at an example smb.conf file:

```
[global]
         workgroup = SAMBA
         encrypt passwords = Yes
         wins support = Yes

[homes]
         comment = Home Directories
         read only = No
         browseable = No

[printers]
         comment = All Printers
         path = /usr/spool/samba
         printable = Yes
         browseable = No

[temp]
         comment = Temporary storage space
         path = /tmp
         read only = No
```

As you can see, there are very few parameters that need to be changed from the defaults. Granted, there are many more that can be set to customize your configuration.

3.3.1 Global parameters

The smb.conf file begins with global settings for the Samba server:

```
[global]
workgroup = SAMBA
encrypt passwords = Yes
wins support = Yes
```

The parameters are described in Table 2.

Table 2. Global parameters

Parameter	Description
workgroup	This parameter specifies in which Windows workgroup or domain the Samba server will participate. If you have an existing Windows network, use its workgroup or domain name for this parameter.
encrypt passwords	Setting this parameter to yes will enable Samba to use the encrypted password protocol when authenticating users. Most newer clients (Windows NT post Service Pack 3, Windows 98 and so on) default to using encrypted passwords.

Parameter	Description
wins support	Setting this parameter to yes allows Samba to become a NetBIOS Name Server (NBNS). If you already have a WINS server on your network, set this to no and set the wins server parameter.

3.3.2 Share parameters

After the global settings for the Samba server come the share parameters. Most share parameters can apply to any share. These parameters are shown in Table 3.

Table 3. Share parameters

Parameter	Description
comment	This can be any string you want, but is usually used to describe the share.
path	Defines the full path to the directory to be shared.
read only	If this is set to yes, then you will not be able to write to the share.
browseable	When set to yes, the share will be visible when browsing the network.

However, there are some parameters that only apply to printer shares. The only one we use is described in Table 4.

Table 4. Printing parameters

Parameter	Description
printable	When set to yes, clients may open, write to, and submit spool files on the directory specified for the service.

3.4 Checking the Samba installation

There are two elements you may need to verify to ensure that you have correctly installed and configured the Samba product. The first one is checking that the smb.conf file is correct; the second is that your machine is now acting as a SMB server.

3.4.1 Checking the smb.conf file

Once the smb.conf file is modified to reflect your environment, you should run the provided test program to test whether 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. Note that SWAT will also do some basic error checking.

The following is an example of the screen output of the testparm program.

```
/usr/local/samba/bin/testparm
Load smb config files from /usr/local/samba/lib/smb.conf
Processing section "[test]"
Processing section "[netlogon]"
Processing section "[utils]"
Loaded services file OK.
Press enter to see a dump of your service definitions
```

Notice the final line of output displays `Loaded services file OK`. This is your indication that the smb.conf file is valid.

3.4.2 Checking your server

If your machine is correctly installed and configured, it is now able to act as a SMB server and provide information about the available shares. The command used to obtain the information is `smbclient` as follows:

```
/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.

When the `testparm` and `smbclient` commands return positive results and the smbd process is running, you should have a properly-functioning Samba server.

Chapter 4. Client configuration

Now that we have seen how to configure and start the Samba server, we can start the client configuration. In this chapter, we will cover how to configure Windows 95/98, Windows NT, Windows 2000, and OS/2 clients to access the Samba server. We will also show how you can use the smbclient program to access files and printers and send and receive Windows pop-up messages. The smbtar program will be discussed as well.

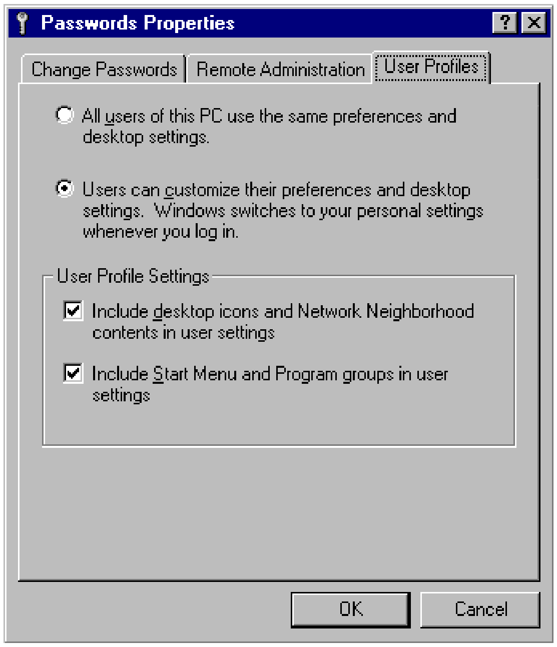
4.1 Accessing Samba from Windows 95 and Windows 98

Let us start with configuring and using Windows 95 and Windows 98 clients (referred to as Windows 9x in this chapter) to access the Samba server.

4.1.1 Windows 9x

Windows 9x was not designed to have multiple users; so, we need to customize it in order to have at least one different profile for each user.

Click **Start -> Settings -> Control Panel** and double-click the **Passwords** icon. The Passwords Properties dialog box appears as shown in Figure 10 on page 30.



○ All users of this PC use the same preferences and desktop settings.

● Users can customize their preferences and desktop settings. Windows switches to your personal settings whenever you log in.

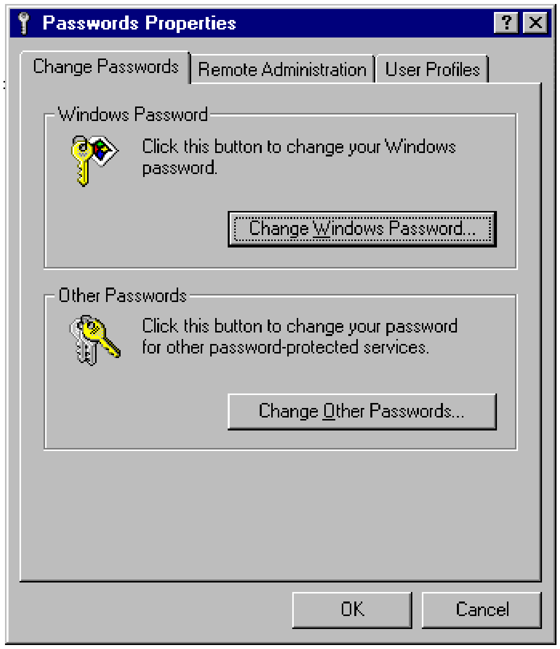
User Profile Settings

☑ Include desktop icons and Network Neighborhood contents in user settings

☑ Include Start Menu and Program groups in user settings

Figure 10. User profiles

Select the **User profiles** tab, and then click the lower of the two radio buttons. Now, click the **Change Passwords** tab. You should see the tab as shown in Figure 11 on page 31.



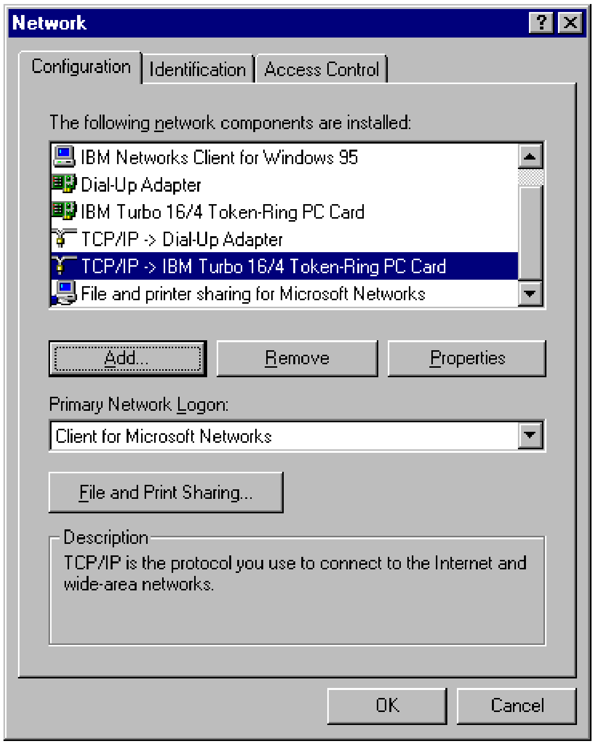
Click this button to change your Windows password.

Click this button to change your password for other password-protected services.

Figure 11. Change Windows passwords

In this tab, you can change the password that you are going to use with the Samba server. If this tab does not appear, you need to reboot Windows, and, when it starts, log on with a user name and password.

Return to the Control Panel and select the **Network** icon. You should now see the Network dialog box shown in Figure 12 on page 32.



The following network components are installed:

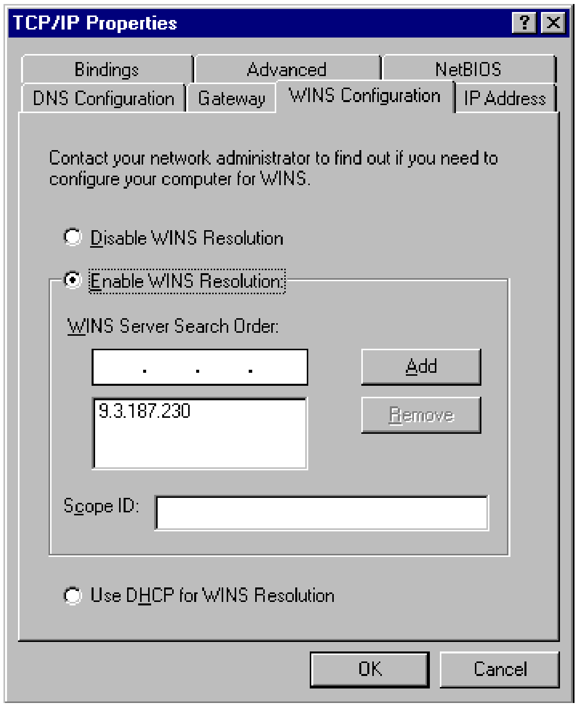
- IBM Networks Client for Windows 95
- Dial-Up Adapter
- IBM Turbo 16/4 Token-Ring PC Card
- TCP/IP -> Dial-Up Adapter
- TCP/IP -> IBM Turbo 16/4 Token-Ring PC Card
- File and printer sharing for Microsoft Networks

Primary Network Logon:
Client for Microsoft Networks

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

Figure 12. Network dialog box

Choose the TCP/IP protocol with the adapter with which that you want to access the Samba server, and click **Properties**. Select the **WINS Configuration** tab, and you should now see the dialog box shown in Figure 13 on page 33.



Contact your network administrator to find out if you need to configure your computer for WINS.

○ Disable WINS Resolution

● Enable WINS Resolution:

WINS Server Search Order:

9.3.187.230

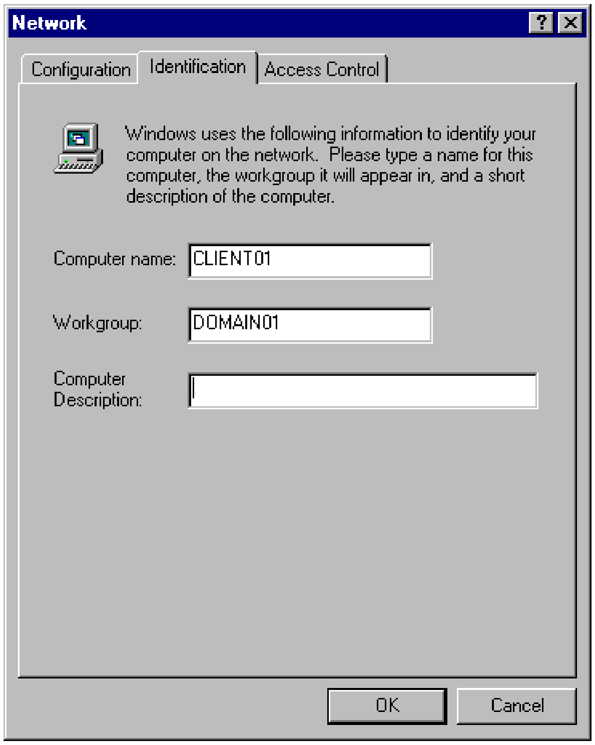
Scope ID:

○ Use DHCP for WINS Resolution

Figure 13. WINS configuration

Click the **Enable WINS Resolutions** radio button. Now, you have to enter the IP Address of the WINS server. Click **Add** and then **OK**.

You should see the Network dialog box again; so, select the **Identification** tab. You should see a dialog box similar to Figure 14 on page 34.



Windows uses the following information to identify your computer on the network. Please type a name for this computer, the workgroup it will appear in, and a short description of the computer.

Computer name: CLIENT01

Workgroup: DOMAIN01

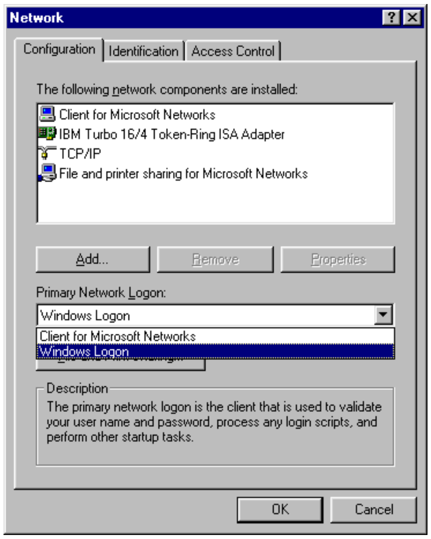
Computer Description:

Figure 14. Windows 95/98 Identification

Enter your Computer name and Workgroup. Put the same workgroup that you have configured in your Samba server. Click **OK** after you enter your Computer name and Workgroup. You will need to reboot in order for your changes to take effect.

4.1.2 Accessing the Samba server

You must have a valid Windows logon to get access to the Samba server. See Figure 15 on page 35 for information on how to select the primary network logon to be a valid logon session.



The following network components are installed:

- Client for Microsoft Networks
- IBM Turbo 16/4 Token-Ring ISA Adapter
- TCP/IP
- File and printer sharing for Microsoft Networks

Primary Network Logon: Windows Logon

- Client for Microsoft Networks
- Windows Logon

Description

The primary network logon is the client that is used to validate your user name and password, process any login scripts, and perform other startup tasks.

Figure 15. Select Primary Network logon

4.1.3 Locating the Samba server from Windows 9x

There are many ways to access the Samba server from standard Windows 9x clients. We will focus on three of these ways:

- Using the Network Neighborhood option
- Using the Find Computer option
- Using the command line

We will use the following parameters in this chapter:

- Domain name: LV200
- Samba servers: lva200a, lva200b
- NetBIOS name server (NBNS): lva200a

4.1.3.1 Using the Network Neighborhood program

The Network Neighborhood option comes standard with all Windows versions. This option is added to the station desktop after the network configuration is done.

Perform the following steps to locate the Samba server through the Network Neighborhood program:

1. Double-click on the **Network Neighborhood** icon.

2. Double-click on the **Entire Network** icon.
3. Double-click on the **Microsoft Windows Network** icon.
4. Select the correct domain name (LVA200) and double-click.
5. You will see the server name (lva200a) and other machines of the same domain as shown in Figure 16.

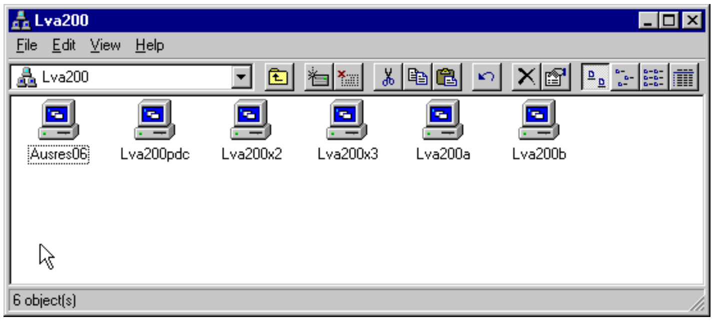
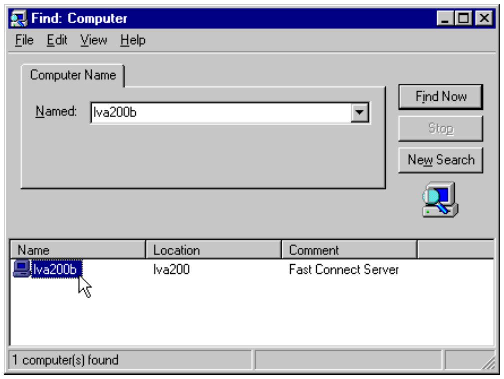


Figure 16. LVA200 domain

4.1.3.2 Using the Find Computer option

Another way to locate the Samba server is by using the Find Computer option. To find the Samba server (lva200b) using this option, perform the following steps:

1. Select the find **Computer** option from the **Find** menu located in the **Start Menu** of Windows 9x (**Start -> Find -> Computer**).
2. Enter the NetBIOS name of the Samba server to locate as shown in Figure 17.



Named: lva200b

Name	Location	Comment
lva200b	lva200	Fast Connect Server

1 computer(s) found

Figure 17. Find Computer

3. Select the ***Find Now*** option and the Samba server will appear.

4.1.3.3 Using the command line

To locate the Samba server from the command line interface, use the `NET VIEW` command in the command line window. The `NET VIEW` command displays a list of computers in the specified domain or shared resources available on the specified computer.

To find the Samba server (lva200a) using this option, perform the following steps:

1. Open an MS-DOS command line interface by selecting **Start -> Programs -> Command Prompt**.
2. Enter the following command to locate the Samba server (lva200a), and you will see a list of shared resources on this server:

```
net view \\<servername>
```

Replace <servername> with the NetBIOS name of the server that you want to locate.

```
C:\WINDOWS>net view \\lva200a
Shared resources at \\lva200a

Samba Server

Share name        Type         Used as      Comment
-------------------------------------------------------------------------------
3130TXT           Printer                   3130 Text printer
HOME              Disk                      User's Home Directory Share
NETLOGON          Disk                      Netlogon Share
PROFILES          Disk                      Profiles Share
TEST              Disk                      Test Directory Share
```

Or enter:

```
net view /DOMAIN:<domainname>
```

Replace `<domainname>` with the domain name that you want to locate.

```
C:\WINDOWS>net view /domain:lva200
Server Name           Remark

-------------------------------------------------------------------
\\AUSRES06
\\LVA200A             43P Samba
\\LVA200B             Samba Server
\\LVA200PDC
\\LVA200X2
\\LVA200X3
The command completed successfully.
C:\>
```

If you use the `net view` command without any parameters, you will see a list of NetBIOS computer names in the network and remarks.

Note

Use the `Net /?` command to see all available options to use with the `NET` command.

4.1.4 Accessing resources from the Samba server

This section describes how to access the Samba server resources, such as files and printers using Windows 9x clients.

4.1.4.1 Accessing files

To access files from shared directories on the Samba server, you can use the GUI interface or the command line interface.

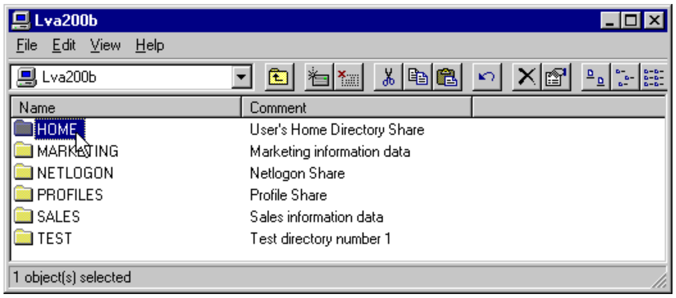
GUI interface

This section describes the process needed to access network share resources using the GUI interface. This process requires the use of Universal Naming Convention (UNC) names. There are two possible ways:

Using a UNC name

You can use UNC names directly through the Network Neighborhood, Windows Explorer, or Run options to access shared resources from Samba servers. Perform the following steps to access files located on shared directories with the Network Neighborhood and Run options:

1. After having located the Samba server (see Section 4.1.3, “Locating the Samba server from Windows 9x” on page 35), double-click on the server, and select the shared folder where your files reside. See Figure 18 on page 39.



Name	Comment
HOME	User's Home Directory Share
MARKETING	Marketing information data
NETLOGON	Netlogon Share
PROFILES	Profile Share
SALES	Sales information data
TEST	Test directory number 1

1 object(s) selected

Figure 18. Shares resources on Samba server

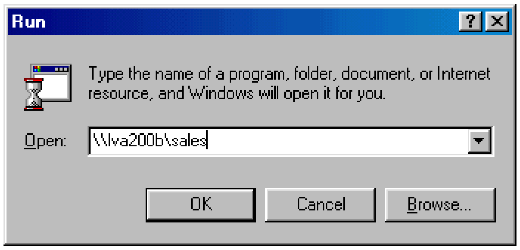
or

2. Select the **Run** option from Start menu and enter the following command using this syntax:

   `\\<ServerName>\<SharedResource>\[Path]`

   Where:

- `<ServerName>` is the NetBIOS name of the Samba server.
- `<SharedResource>` is the shared name.
- `[Path]` is the path where the files reside. See Figure 19.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: \\lva200b\sales

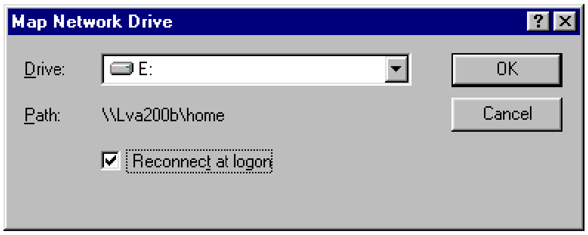
Figure 19. Run command window

Mapping network drive

Some applications do not have good performance or do not support the use of UNC names to access shared resources. In this case, it is necessary to create logical drives where the UNC name is mapped to an available drive letter. Perform the following steps to map a network drive:

1. Locate the server and share name where the files reside.
2. Select the shared resource and select the **Map Network Drive** option from the File menu or by right-clicking on it.

3. Select an available drive letter to which to link the UNC name and check the Reconnect at Logon option to make this map available every time the machine is restarted. See Figure 20.



Drive: E:

Path: \\Lva200b\home

☑ Reconnect at logon

Figure 20. Map Network Drive window

Command line interface

With the command line interface, the only way to access shared resources from the Samba server is by mapping the UNC name to a drive letter. To map drives from the command line, use the `NET USE` command.

```
C:\>net use d: \\lva200a\home
The command completed successfully.

C:\>
```

Use the `Net help` command to see more information about the `Net` command.

4.1.4.2 Accessing Printer shares

To access printers located in the Samba server acting as a print server, it is required to add this printer and install the appropriate printer driver.

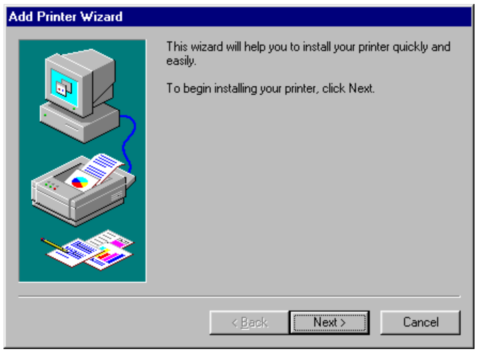
There are two ways of configuring a network printer in Windows 9x:

- Using the GUI interface.
- Using the command line interface.

GUI interface

Perform the following steps to configure a network printer located in the Samba server:

1. Select the **Printers** administration folder from Start menu or My Computer icon: **Start -> Settings -> Printers** or **My Computer -> Printers**.
2. Double-click on the **Add Printer** icon to create a new printer. The ***Add*** Printer Wizard will appear as shown in Figure 21 on page 41.

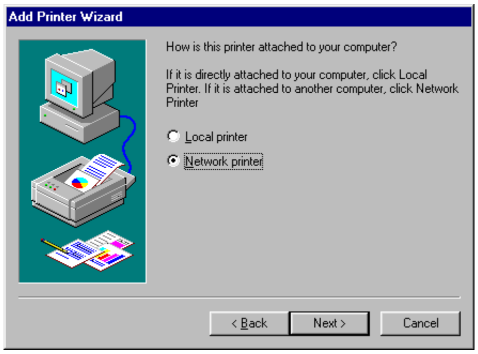

Add Printer Wizard

This wizard will help you to install your printer quickly and easily.

To begin installing your printer, click Next.

Figure 21. Add Printer Wizard

3. Press the **Next** button and select the type of connection with the printer. In this case, it is a **Network printer** as shown in Figure 22.


Add Printer Wizard

How is this printer attached to your computer?

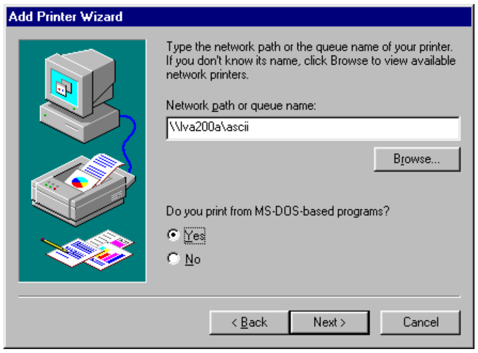
If it is directly attached to your computer, click Local Printer. If it is attached to another computer, click Network Printer

○ Local printer

● Network printer

Figure 22. Select printer connection method window wizard

4. Press the **Next** button and enter the network path where this printer is located (UNC). Select the **Yes** or **No** radio button option if you want to use this printer from MS-DOS based programs. See Figure 23 on page 42.



Add Printer Wizard

Type the network path or the queue name of your printer. If you don't know its name, click Browse to view available network printers.

Network path or queue name:

\\lva200a\ascii

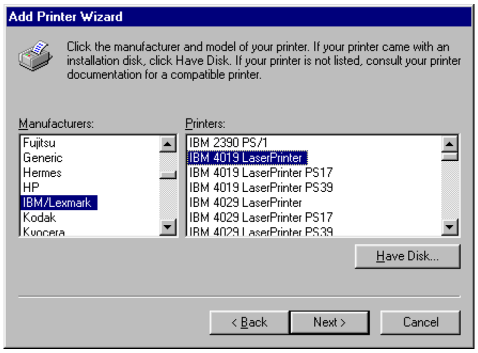
Do you print from MS-DOS-based programs?

● Yes

○ No

Figure 23. Enter network printer path

5. Press the **Next** button and select the printer driver that will be used with this printer. You may have to provide the CDROM containing this driver during this step. See Figure 24.



Add Printer Wizard

Click the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for a compatible printer.

Manufacturers:

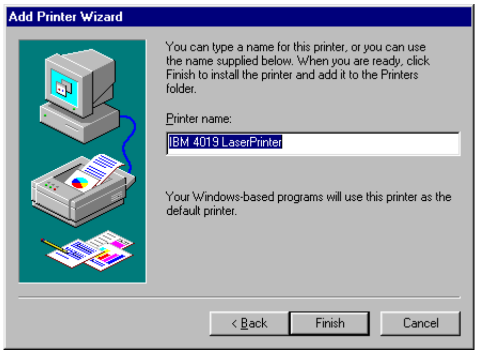
Fujitsu
Generic
Hermes
HP
IBM/Lexmark
Kodak
Kyocera

Printers:

IBM 2390 PS/1
IBM 4019 LaserPrinter
IBM 4019 LaserPrinter PS17
IBM 4019 LaserPrinter PS39
IBM 4029 LaserPrinter
IBM 4029 LaserPrinter PS17
IBM 4029 LaserPrinter PS39

Figure 24. Select printer driver

6. Press **Next** and enter the printer name for your client. See Figure 25 on page 43.



Add Printer Wizard

You can type a name for this printer, or you can use the name supplied below. When you are ready, click Finish to install the printer and add it to the Printers folder.

Printer name: IBM 4019 LaserPrinter

Your Windows-based programs will use this printer as the default printer.

Figure 25. Set printer name

7. Press the **Finish** button. The printer is now ready to be used from any Windows program.

Command line interface

To access a printer located on the Samba server from the command line, it is required to map the UNC name of the printer with an available LPT port . Use the following command to map a network printer from the command line:

```
net use LPT1: \\lva200a\ascii
```

You will then have to follow the steps described in “GUI interface” on page 40 to associate a driver and a name to this printer.

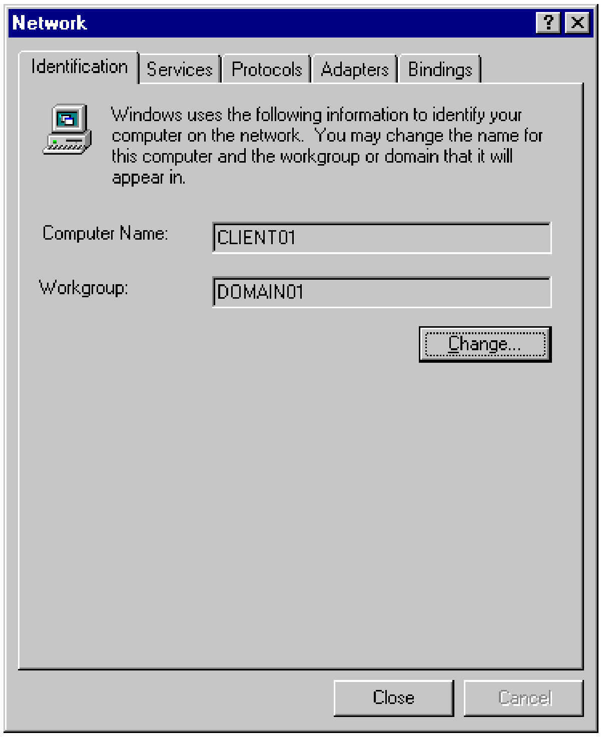
4.2 Accessing Samba from Windows NT clients

This section will describe how to access shared resources, such as files and printers, from Samba server using Windows NT client.

4.2.1 Configuring Windows NT

Before you start to configure Windows NT, make sure that you have installed the Workstation service and the TCP/IP protocol. Make sure that you are logged on as Administrator or at least with a user that is included in the local Administrators group.

Click on **Start -> Settings -> Control Panel** and double-click on the **Network** icon. The Network dialog box should appear as shown in Figure 26 on page 44.



Network

Identification | Services | Protocols | Adapters | Bindings

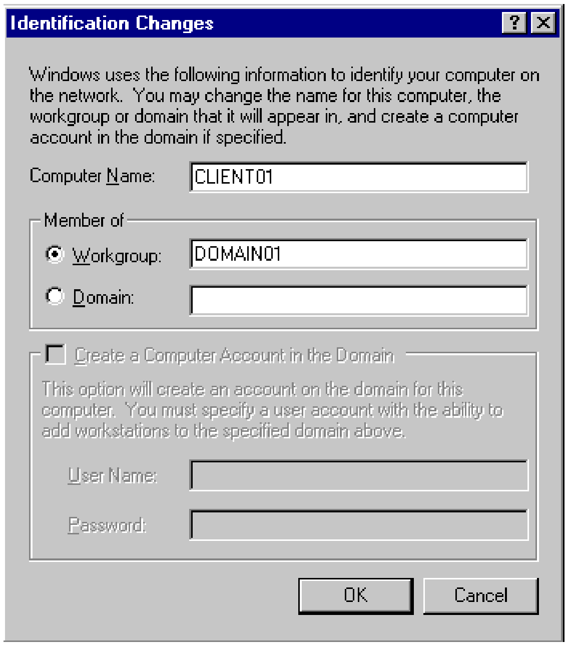
Windows uses the following information to identify your computer on the network. You may change the name for this computer and the workgroup or domain that it will appear in.

Computer Name: CLIENT01

Workgroup: DOMAIN01

Figure 26. Windows NT Identification

While on the Identification tab, click the **Change** button, and you will see the dialog box shown in Figure 27 on page 45.



Identification Changes

Windows uses the following information to identify your computer on the network. You may change the name for this computer, the workgroup or domain that it will appear in, and create a computer account in the domain if specified.

Computer Name: CLIENT01

Member of

● Workgroup: DOMAIN01

○ Domain:

□ Create a Computer Account in the Domain

This option will create an account on the domain for this computer. You must specify a user account with the ability to add workstations to the specified domain above.

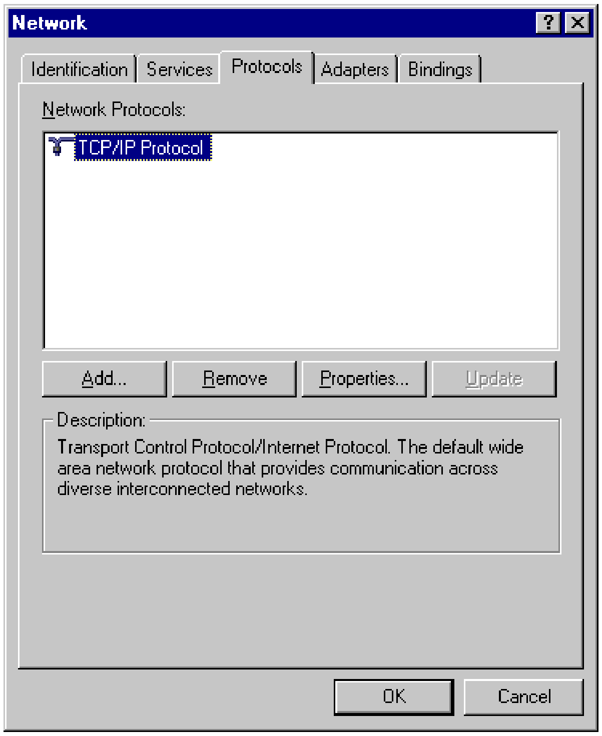
User Name:

Password:

Figure 27. Identification Changes

You should first enter your Computer Name. You will see that you will not be able to change the Workgroup at this moment in time; so, you have to click **OK**, and then click the **Change** button again to return to the Identification Changes dialog box. Now, you should click the **Workgroup** radio button and enter your Workgroup name. Put the same workgroup name that you have set up in your Samba server. You can use the same Computer Name that you enter in your TCP/IP configuration. Click **OK** when finished.

You should now be back in the Network dialog box. If you have set up your Samba server to provide WINS service, you can configure the WINS Address. Click the **Protocols** tab on the Network dialog box, and you should see a dialog box similar to the one shown in Figure 28 on page 46.



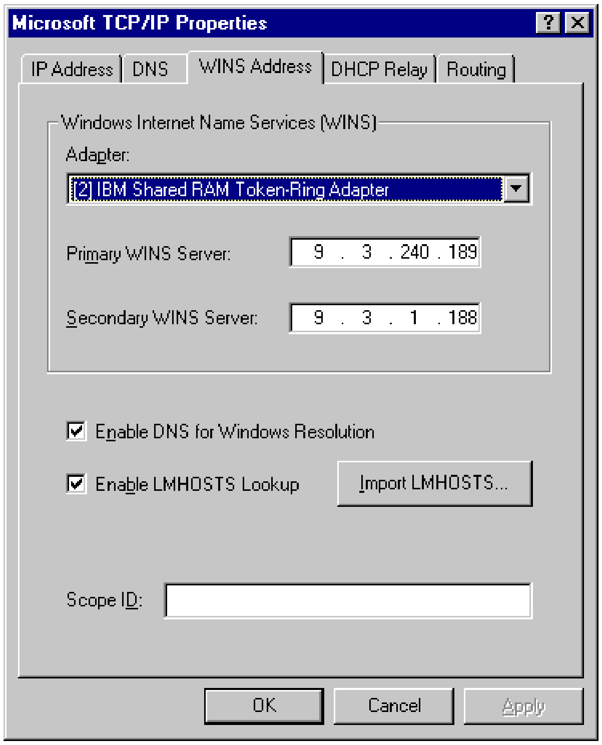
Network Protocols:

TCP/IP Protocol

Description:
Transport Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Figure 28. Protocols

Select **TCP/IP Protocol** and click **Properties**. You should see the TCP/IP dialog box. Select the **WINS Address** tab, and you will see the dialog box shown in Figure 29 on page 47.



Microsoft TCP/IP Properties

Windows Internet Name Services (WINS)

Adapter: [2] IBM Shared RAM Token-Ring Adapter

Primary WINS Server: 9 . 3 . 240 . 189

Secondary WINS Server: 9 . 3 . 1 . 188

☑ Enable DNS for Windows Resolution

☑ Enable LMHOSTS Lookup

Scope ID:

Figure 29. WINS Address

Enter the IP address of your Samba server as the Primary WINS Server. You can check the **Enable DNS for Windows Resolution** box. This way, if your client cannot find a name, it will try to use the DNS. Click **OK** on the WINS Address tab and **OK** on the Network dialog box. You will need to reboot in order for the changes to take effect.

4.2.2 Locating the Samba server

There are three ways to locate a Samba server from Windows clients:

- Through the Network Neighborhood icon
- Through the Find Computer option
- Through the Command Line

In this chapter, we will use LVA200 as the domain name and the NetBIOS server name, \\LVA200A.

4.2.2.1 Locating the server through the Network Neighborhood

Perform the following steps:

1. Double-click on the **Network Neighborhood** icon.
2. Double-click on the **Entire Network** icon.
3. Double-click on the **Microsoft Windows Network** icon.
4. Double-click on the domain of your Samba server (see Figure 30).

You will find the servers on the domain you have selected.

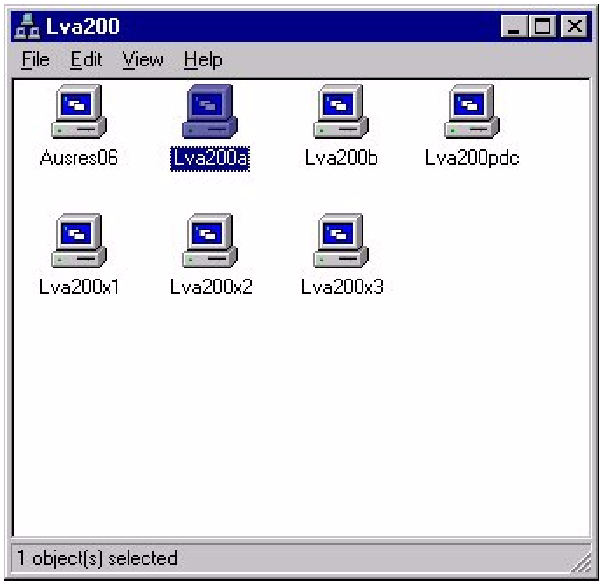
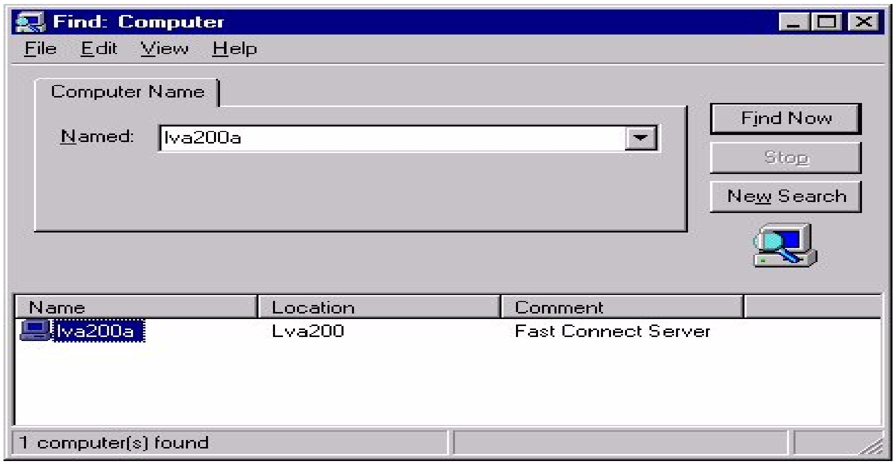


Figure 30. Browsing the LVA200 domain

4.2.2.2 Locating the server with the Find: Computer option

You can use the Find: Computer option to find the Samba server on the network. Perform the following steps:

1. Select **Start -> Find -> computer**.
2. Type the computer name (see Figure 31 on page 49)
3. Click on **Find Now**.



Named: lva200a

Name	Location	Comment
lva200a	Lva200	Fast Connect Server

1 computer(s) found

Figure 31. Find: Computer

4.2.2.3 Locating the server from the command line

You can locate the Samba server with the `net view` command. The `net view` command displays a list of computers in the specified domain or shared resources available on the specified computer.

1. Select **Start -> Programs -> MS-DOS Command Prompt**.
2. At the command prompt, type: `net view \\<servername>` (`servername` is the name of the Samba server whose resources you want to view), or type `net view /DOMAIN:<domainname>` (`domainname` is the name of the domain of your Samba server).

```
C:\>net view \\lva200a
Shared resources at \\lva200a

Samba Server

Share name   Type         Used as  Comment

-------------------------------------------------------------------------------
ASCII        Print
HOME         Disk         H:       User's Home Directory Share
NETLOGON     Disk                  Netlogon Share
PROFILES     Disk         I:       Profile Share
TMP          Disk         K:
The command completed successfully.


C:\>
```

If you use the `net view` command without command-line parameters, you see a list of computers with computer names in the left column and remarks in the right column.

If you use the `net view` command with a NetBIOS computer name (Windows server), you will see a list of available resources on that computer.

Note

You can use the `net view` command to accomplish most of the performing tasks available in Network Neighborhood, except that you cannot view a list of workgroups.

4.2.3 Accessing resources from the Samba server

The following sections describe how to connect Windows NT clients to the Samba server.

4.2.3.1 Accessing files

You can access the Samba shares from your Windows NT client with either the GUI interface or the command line interface.

Using the GUI interface

When you want to access the network share from your Windows NT client, you must create a mapping to this share. You can use the Network Neighborhood icon or the Find Computer panel to do this.

In this example, we use the Find Computer option. You can follow these steps to map a network drive to a Samba shared resource:

1. Click **Start -> Find -> Computer**.
2. Enter the Computer Name and click on **Find Now** (see Figure 31 on page 49).
3. Double-click on the computer name (in this example, the computer name is lva200a)
4. You will see the shared resources of lva200a server in a new window (see Figure 32 on page 51).

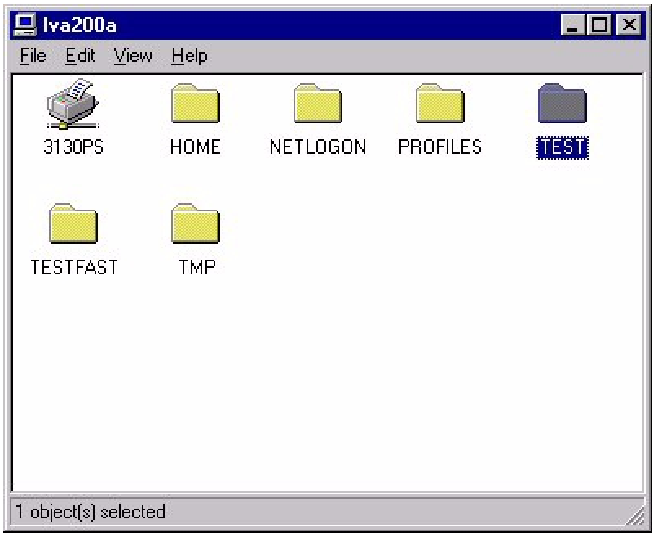
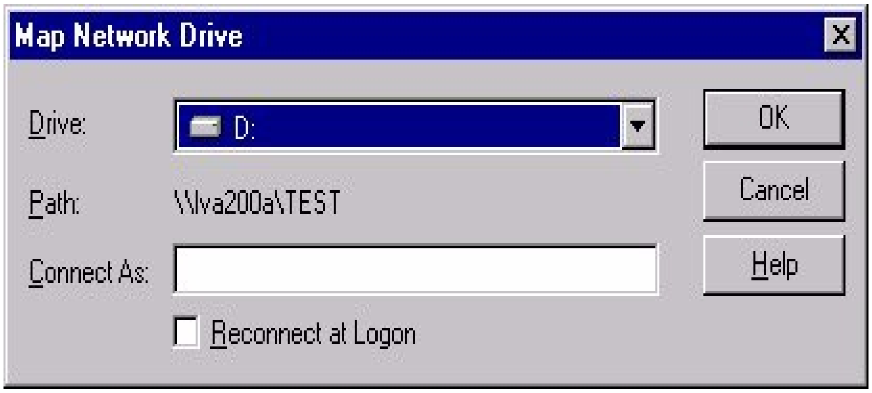


Figure 32. Samba shares

5. Click on the shared resource (for example, TEST) and select **File -> Map Network Drive..** or right-click on the shared resource and select **Map Network Drive...**
6. Select the desired drive (for example **D**:)
7. Click **OK** (see Figure 33).



Drive: D:

Path: \\lva200a\TEST

Connect As:

□ Reconnect at Logon

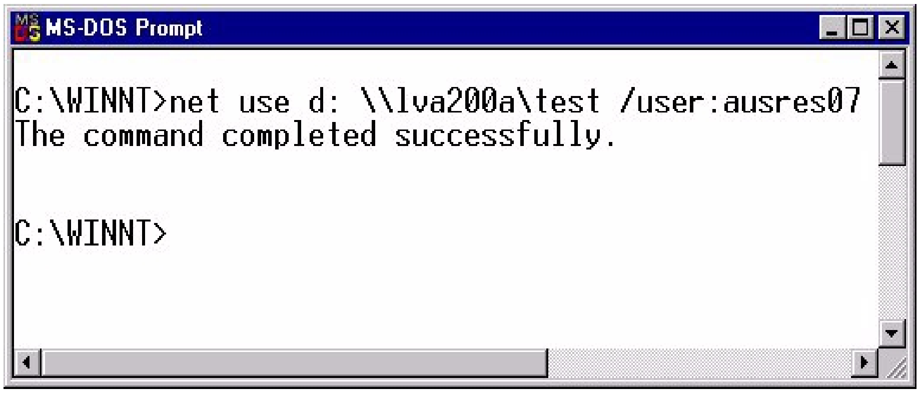
Figure 33. Map Network Drive

Command line interface

Windows NT will need to define a drive mapping to access the shared resources exported by Samba. These drive mappings can be done from the DOS command prompt.

You have to use the `NET USE` command to define mappings between PC drive letters and a Samba shared resource:

DOS> `net use D: \\lva200a\test /user:<user_name>`



```
C:\WINNT>net use d: \\lva200a\test /user:ausres07
The command completed successfully.


C:\WINNT>
```

Figure 34. Map network drive from MS-DOS

DOS> `net help` (help info for net command)

DOS> `net use D: /delete` (delete the drive mapping)

If you use the `NET USE` command without command-line parameters, you see the status of network connections, the local name of connections (the mapped drive letters), and the remote name of connections (the server location).

4.2.3.2 Accessing the Samba printers

If you want to access a Samba server printer from Windows NT, you will need to install the appropriate printer driver and map the print resource to a network printer.

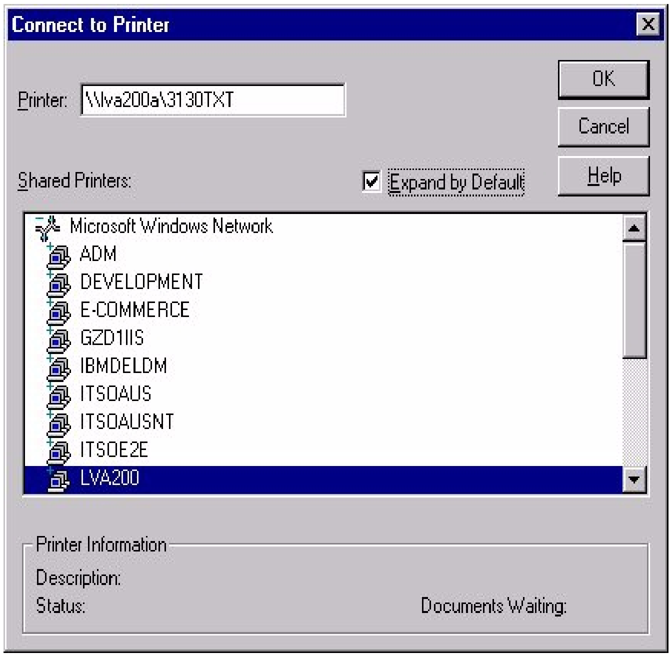
You have two ways to configure a network printer on Windows NT:

- From the GUI interface
- From the command line interface

GUI interface

you can follow this procedure to configure a network printer from the GUI interface:

1. Select **Start -> Settings -> Printers -> Add Printer**.
2. Select **Network printer server**.
3. Select the network printer from a list or enter its path directly (for example, :\\lva200a\3130TXT as shown in Figure 35).



Connect to Printer

Printer: \\lva200a\3130TXT

Shared Printers:

☑ Expand by Default

Microsoft Windows Network
ADM
DEVELOPMENT
E-COMMERCE
GZD1IIS
IBMDELDM
ITSOAUS
ITSOAUSNT
ITSOE2E
LVA200

Printer Information
Description:
Status:
Documents Waiting:

Figure 35. Connect to Printer

4. Select the proper Windows printer driver from the list (for example, select **Lexmark Optra N**) and install it from the Windows installation media (see Figure 36 on page 54).

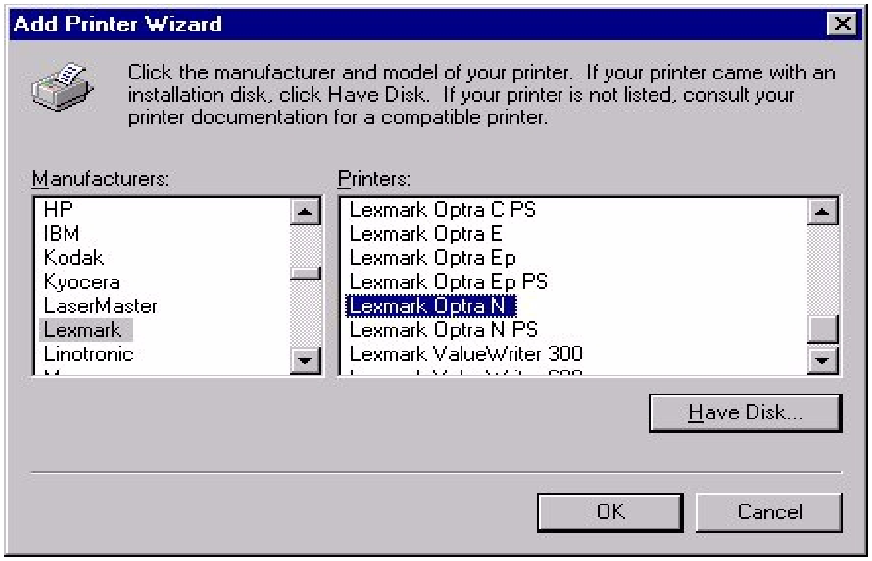


Figure 36. Add Printer Wizard

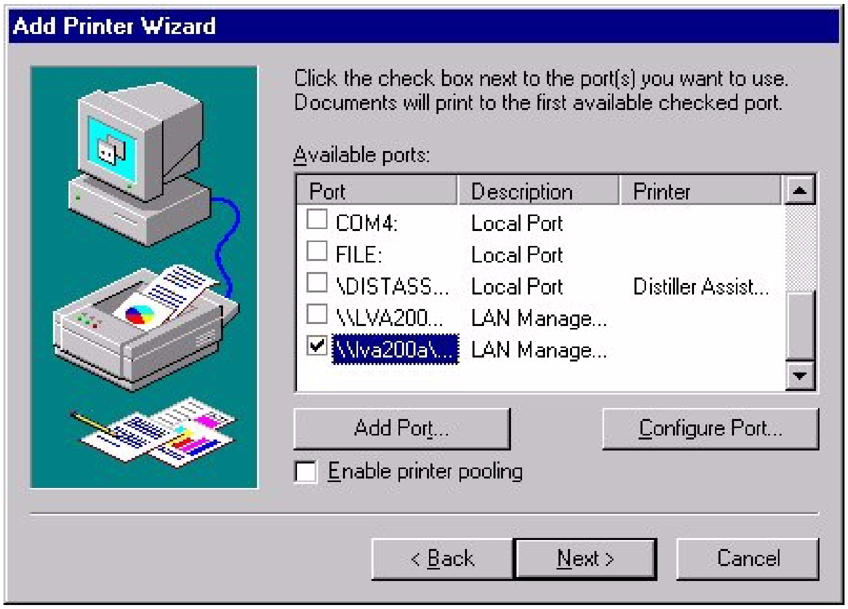
Command line interface

For DOS applications, you can map the network printer to local printer devices (for example LPT1). You can use the following simple device mapping on Windows NT client:

```
DOS> net use LPT1: \\lva200a\3130TXT
```

If you want to print from a Windows application, a Windows printer driver must be installed and mapped to the network printer. You must perform the following steps:

1. Select **Start -> Settings -> Printers -> Add Printer**.
2. Select **My Computer**.
3. Click the check box next to the port you want to use (see Figure 37 on page 55).



Click the check box next to the port(s) you want to use. Documents will print to the first available checked port.

Available ports:

	Port	Description	Printer
☐	COM4:	Local Port	
☐	FILE:	Local Port	
☐	\DISTASS...	Local Port	Distiller Assist...
☐	\\LVA200...	LAN Manage...	
☑	\\lva200a\...	LAN Manage...	

☐ Enable printer pooling

Figure 37. Select port

4. Select the proper Windows driver from the list (for example, select **Lexmark Optra N**) and install it from the Windows installation media (see Figure 36 on page 54).

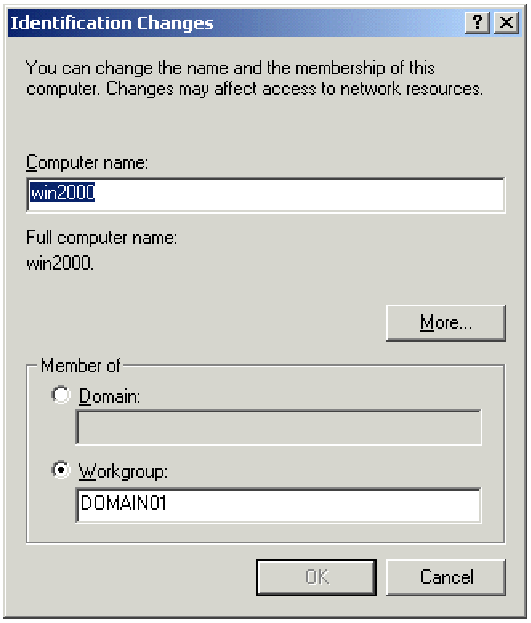
4.3 Access the Samba server from Windows 2000

This section describes how to access shared resources, such as files and printers, from a Samba server using Windows 2000 clients.

4.3.1 Configuring Windows 2000

Before you start to configure Windows 2000, make sure that you have installed the Workstation service and the TCP/IP protocol. Make sure that you are logged on as Administrator or at least with a user that is included in the local Administrators group. Perform the following steps:

1. Click on **Start -> Settings -> Control Panel** and double-click the **System** icon. The System Properties dialog box should appear.
2. Select the **Network Identification** tab, and click the **Properties** button. You should see a dialog box as shown in Figure 38 on page 56.


Identification Changes

You can change the name and the membership of this computer. Changes may affect access to network resources.

Computer name: win2000

Full computer name: win2000.

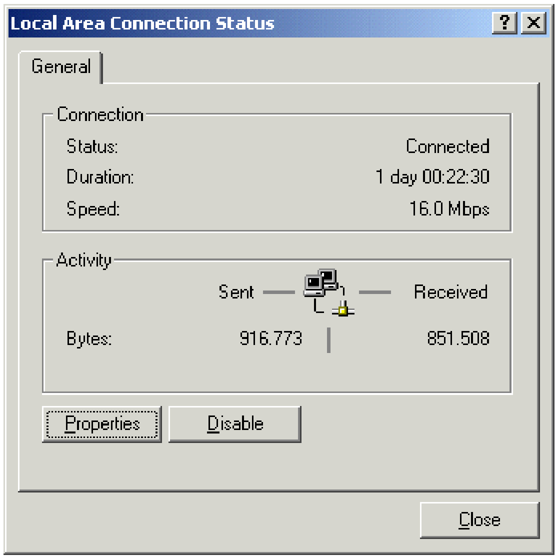
Member of

○ Domain:

● Workgroup: DOMAIN01

Figure 38. Identification Changes

3. Enter your computer name. Next, you have to click the radio button for **Workgroup** and enter the workgroup name. The workgroup name should match with the one that you set up in your Samba server.
4. Click **OK** to complete this process. Your computer will ask you to reboot. You do not need to reboot now. You can reboot when you finish the setup.
5. Returning to the Control Panel, double-click **Network and Dial-up Connections**, and then double-click the **Local Area Connection** icon. You should see the dialog box shown in Figure 39 on page 57.



Local Area Connection Status

General

Connection

Status: Connected

Duration: 1 day 00:22:30

Speed: 16.0 Mbps

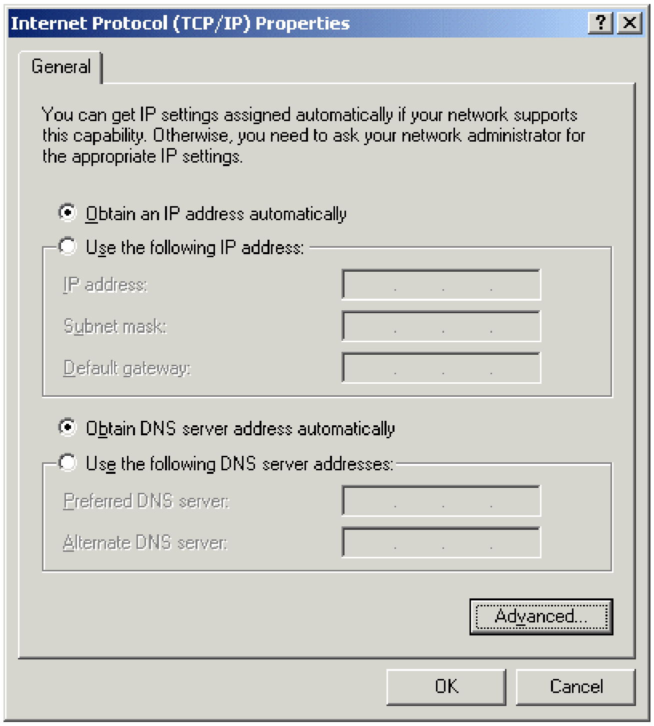
Activity

Sent — Received

Bytes: 916.773 851.508

Figure 39. Local Area Connection Status

6. Click the **Properties** button, and then select **Internet Protocol (TCP/IP)** and click **Properties**. You should see the Internet Protocol (TCP/IP) Properties box dialog box as shown in Figure 40 on page 58.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

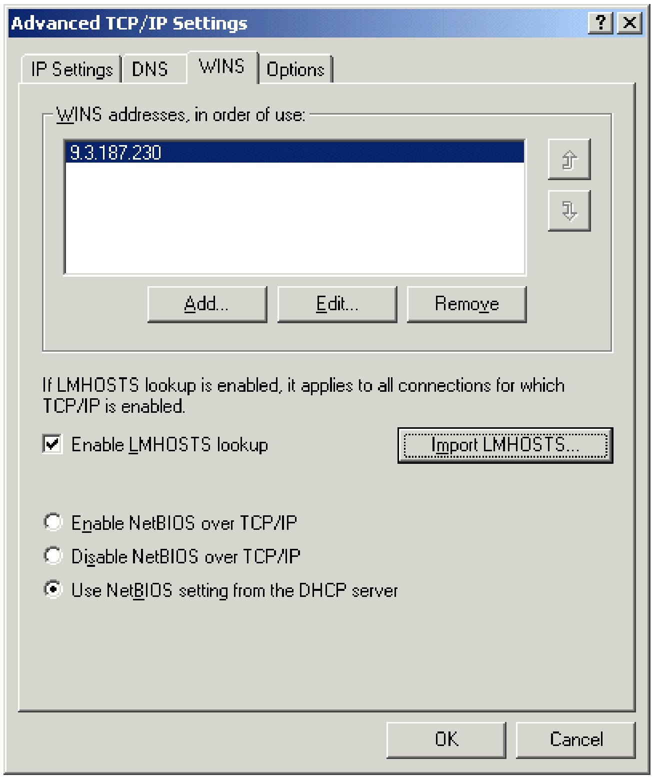
○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

Figure 40. Internet Protocol (TCP/IP) Properties

7. Click the **Advanced** button. You should see the Advanced TCP/IP Settings dialog box. Then, select the **WINS** tab. The screen, shown in Figure 41 on page 59, appears.



WINS addresses, in order of use:

9.3.187.230

If LMHOSTS lookup is enabled, it applies to all connections for which TCP/IP is enabled.

☑ Enable LMHOSTS lookup

○ Enable NetBIOS over TCP/IP

○ Disable NetBIOS over TCP/IP

● Use NetBIOS setting from the DHCP server

Figure 41. Advanced TCP/IP Settings

8. Click **Add**, and enter the IP address of your WINS server. If you have set up your Samba server to provide WINS service, you can enter the IP address of your Samba server in this field.
9. Now, click **OK** in the Advanced TCP/IP settings dialog box, click **OK** in the Internet Protocol (TCP/IP) Properties dialog box, click **OK** in the Local Area Connection Properties, and click **Close** in the Local Area Connection Status dialog box. You will need to reboot in order for the changes to take effect.

4.3.2 Locating the Samba server

There are three ways to locate a Samba server from Windows 2000 clients:

- The My Network Places icon
- The Find Computer option
- The command line

In this chapter, we use the domain name, LVA200, and the NetBIOS server name, lva200a.

4.3.2.1 Locating the server with the My Network Places icon

To locate the server with the My Network Places icon, complete the following steps:

1. Click the **My Network Places** icon.
2. Click the **Entire Network** icon.
3. Click the **Entire Contents** text.
4. Click the **Microsoft Windows Network** icon.
5. Click the domain of your Samba server.

You will find the servers on the domain you have selected as shown in Figure 42.

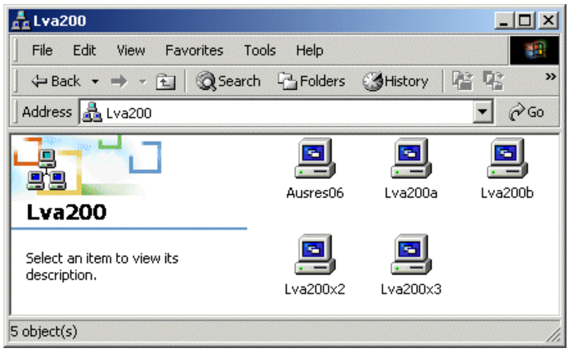
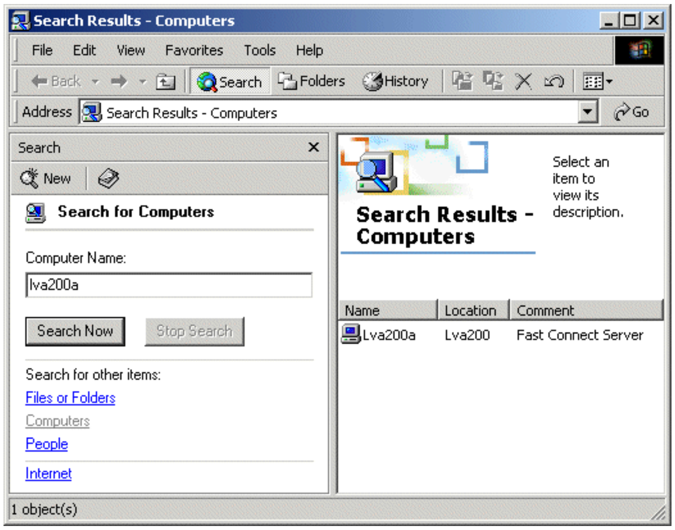


Figure 42. Browsing LVA200

4.3.2.2 Locating the server with the Search for Computer option

You can use the Find computer option to find the Samba server on the network. Complete the following steps:

1. Click the **My Network Places** icon.
2. Click the **Entire Network** icon.
3. Click the **Search for Computer** text.
4. Enter the computer name (see Figure 31 on page 49).
5. Click the **Search Now button** shown in Figure 43 on page 61.


Search Results - Computers
File Edit View Favorites Tools Help
Back Search Folders History
Address Search Results - Computers
Go
Search
New
Search for Computers
Search Now
Stop Search
Search for other items:
Files or Folders
Computers
People
Internet
Search Results - Computers
Select an item to view its description.
1 object(s)

Computer Name: lva200a

Name	Location	Comment
Lva200a	Lva200	Fast Connect Server

Figure 43. Search for Computers

4.3.2.3 Locating the server from the command line

You can locate the server with the `net view` command. The `net view` command displays a list of computers in the specified domain, or shared resources available on the specified computer. Complete the following steps:

1. Select **Start -> Programs -> Accessories -> Command Prompt**.
2. At the command prompt, type: `net view \\<servername>` (`servername` being the name of the Samba server whose resources you want to view), or type `net view /DOMAIN:<domainname>` (`domainname` being the name of the domain of your Samba server).

If you use the `net view` command without command line parameters, you see a list of computers with computer names in the left column and remarks in the right column.

If you use the `net view` command with a NetBIOS computer name (Windows server), you will see a list of available resources on that computer.

Note

You can use the `net view` command to accomplish most of the performing tasks available in Network Neighborhood. However, you cannot view a list of workgroups.

4.3.3 Accessing resources from the Samba server

The following sections describe how to connect a Windows 2000 client to a Samba server.

4.3.3.1 Accessing Files

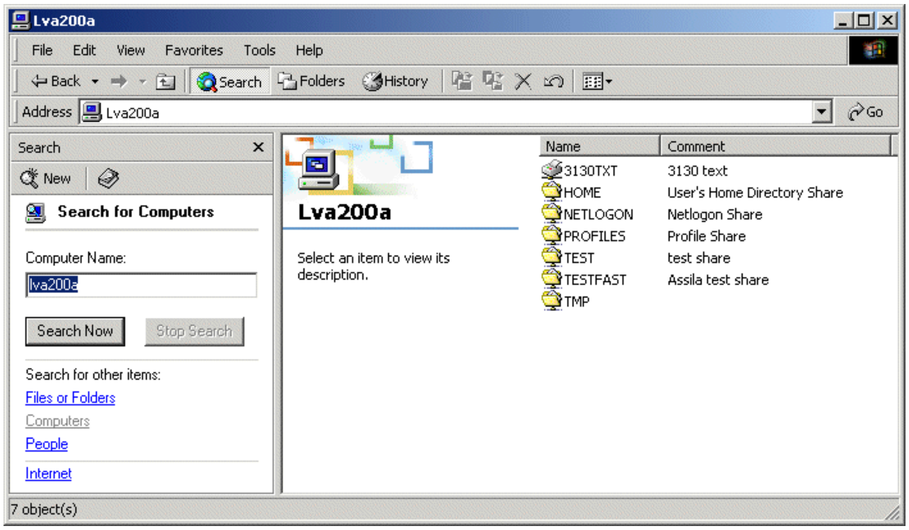
You can access the Samba shares from your Windows 2000 client from the GUI interface or the command line interface.

Using the GUI interface

When you want to access the network shared resource from your Windows 2000 client, you can create a mapping to this shared resource. You can use the My Network Places icon or the Search for Computers panel to do this.

In this example, we use the Search for Computers option. You can perform the following steps to map a network drive to Samba shared resources:

1. Click the **My Network Places** icon.
2. Click the **Entire Network** icon.
3. Click the **Search for Computers** text.
4. Enter the computer name and click the **Search Now** button (see Figure 31 on page 49).
5. Double-click the computer name (lva200a in this example).
6. You will see the shared resources of the lva200a server (see Figure 44).

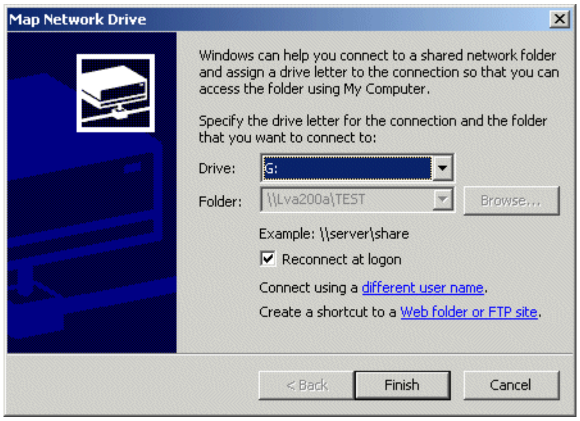


Computer Name: lva200a

Name	Comment
3130TXT	3130 text
HOME	User's Home Directory Share
NETLOGON	Netlogon Share
PROFILES	Profile Share
TEST	test share
TESTFAST	Assila test share
TMP	

Figure 44. Samba shared resources

7. Click the shared resource (for example, TEST) and select **File -> Map Network Drive...** or right-click the shared resource and select **Map Network Drive...**.
8. Select the desired drive (for example **G:**).
9. Click the **Finish** button shown in Figure 33.



Map Network Drive

Windows can help you connect to a shared network folder and assign a drive letter to the connection so that you can access the folder using My Computer.

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: G:

Folder: \\Lva200a\TEST

Example: \\server\share

☑ Reconnect at logon

Connect using a different user name.

Create a shortcut to a Web folder or FTP site.

Figure 45. Map Network Drive

Using the command line interface

Windows 2000 can also define drive mapping to the shared resources from the DOS command prompt.

You have to use the `net use` command to define mappings between the PC drive letters and the Samba shared resource. You can use the `net use` command without parameters to see the current status of mapped shares.

```
C:\> net use
New connections will be remembered.

Status       Local      Remote                    Network
-------------------------------------------------------------------------------
```

In this example, you can see the creation of a network drive, D:, which is connected to share test on the lva200a computer.

```
C:\> net use d: \\lva200a\test /user:ausres07
The command completed successfully.
C:\> net use
New connections will be remembered.

Status       Local     Remote                    Network
-------------------------------------------------------------------------------
OK           D:        \\lva200a\test            Microsoft Windows Network
```

You can delete network mapping with the `/delete` option.

```
C:\> net use d: /delete
The command completed successfully.
C:\> net use
New connections will be remembered.

Status       Local     Remote                    Network
-------------------------------------------------------------------------------
Disconnected P:        \\lva200b\home            Microsoft Windows Network
```

4.3.3.2 Accessing printers

If you want to access a Samba server printer from Windows 2000, you will need to install the appropriate printer driver and map it to the network printer.

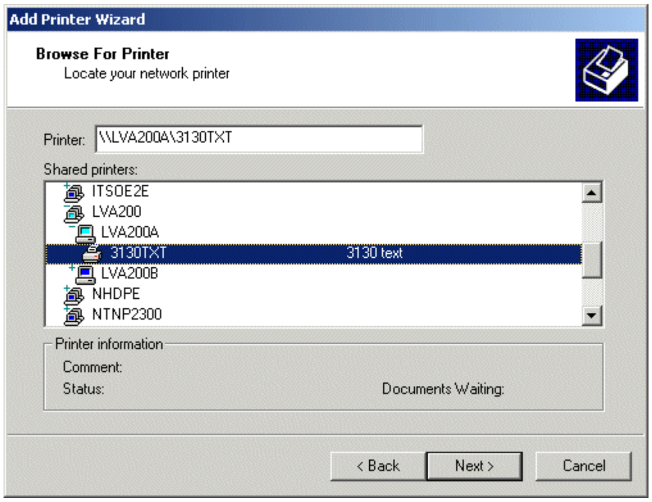
You have two ways of configuring a network printer on the Windows 2000 client:

- From the GUI interface
- From the command line interface

Using the GUI interface

You can perform the following steps to configure a network printer from the GUI interface:

1. Select **Start -> Settings -> Printers -> Add Printer**.
2. Press the **Next** button.
3. Select the Network printer server and press the **Next** button.
4. Select the network printer from a list or enter its path directly (for example, \\lva200a\3130TXT). See Figure 46 on page 65.



Add Printer Wizard

Browse For Printer
Locate your network printer

Printer: \\LVA200A\3130TXT

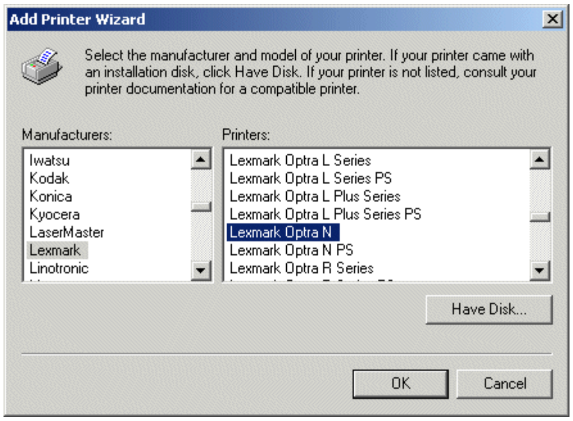
Shared printers:

ITSOE2E
LVA200
LVA200A
3130TXT 3130 text
LVA200B
NHDPE
NTNP2300

Printer information
Comment:
Status: Documents Waiting:

Figure 46. Connect to printer

5. Select the proper Windows printer driver from the list (for example, select **Lexmark Optra N**), and install it from the Windows installation media (see Figure 47).



Add Printer Wizard

Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for a compatible printer.

Manufacturers:	Printers:
Iwatsu	Lexmark Optra L Series
Kodak	Lexmark Optra L Series PS
Konica	Lexmark Optra L Plus Series
Kyocera	Lexmark Optra L Plus Series PS
LaserMaster	Lexmark Optra N
Lexmark	Lexmark Optra N PS
Linotronic	Lexmark Optra R Series

Figure 47. Add Printer Wizard

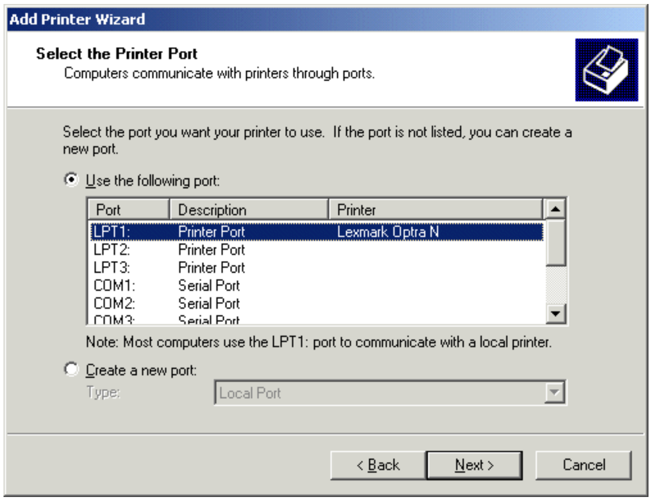
Command line interface

For DOS application, you can map the network printer to local printer devices (for example, LPT1). You can use the following simple device mapping on Windows 2000 client:

```
net use LPT1: \\lva200a\3130txt
```

If you want to print from a Windows application, a windows printer driver must be installed and mapped to the network printer. You must perform the following steps:

1. Select **Start -> Settings -> Printers -> Add Printer**.
2. Click the **Next** button.
3. Select **Local Printer** and deselect **Automatically detect and install my Plug and Play printer** option.
4. Select the port you want to use (see Figure 48), and press the **Next** button.


Add Printer Wizard

Select the Printer Port

Computers communicate with printers through ports.

Select the port you want your printer to use. If the port is not listed, you can create a new port.

● Use the following port:

Port	Description	Printer
LPT1:	Printer Port	Lexmark Optra N
LPT2:	Printer Port	
LPT3:	Printer Port	
COM1:	Serial Port	
COM2:	Serial Port	
COM3:	Serial Port	

Note: Most computers use the LPT1: port to communicate with a local printer.

○ Create a new port:

Type: Local Port

Figure 48. Select a port

5. Select the proper windows driver from the list (for example, select **Lexmark Optra N**) and install it from the windows installation media (see Figure 36 on page 54).
6. Press the **Next** Button.
7. Enter the name of the printer, and press the **Next** button.
8. Press the **Next** button three times, and then press the **Finish** button.

4.4 Accessing Samba from OS/2 clients

This chapter describes how to access shared resources, such as files and printers, from a Samba server using OS/2 clients.

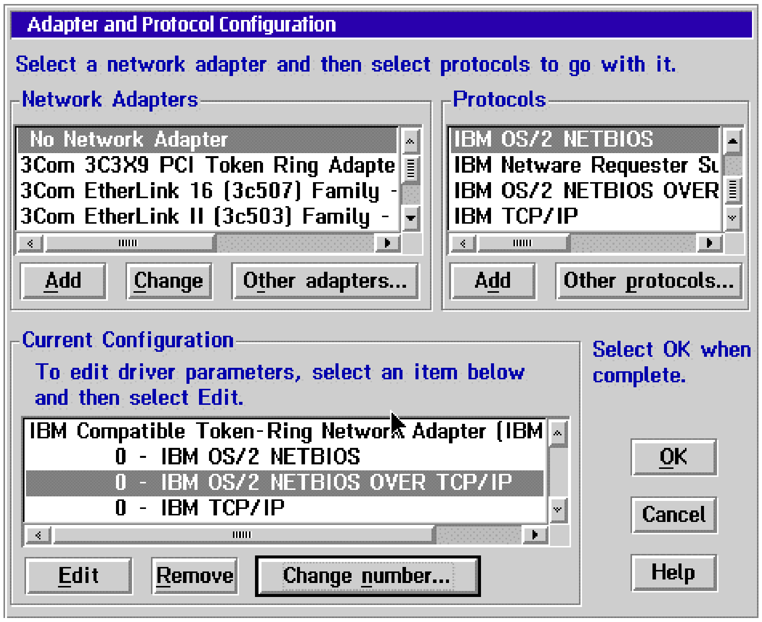
4.4.1 OS/2 configuration

NetBIOS over TCP/IP is required to be set up on your OS/2 machine if you are going to access your Samba server on AIX. As part of the configuration, you will need to update both OS/2 Multiple Protocol Transport Services (MPTS) and Lan Requester as part of this setup.

4.4.1.1 Configuring MPTS

The steps that follow assume the MPTS with TCP/IP are already operational.

1. Double-click the MPTS icon or enter MPTS from an OS/2 window.
   - Click **Configure**.
   - Select **Lan Adapter and Protocols** and click **Configure**. See Figure 49.



Adapter and Protocol Configuration

Select a network adapter and then select protocols to go with it.

Network Adapters

No Network Adapter
3Com 3C3X9 PCI Token Ring Adapte
3Com EtherLink 16 (3c507) Family -
3Com EtherLink II (3c503) Family -

Protocols

IBM OS/2 NETBIOS
IBM Netware Requester Su
IBM OS/2 NETBIOS OVER
IBM TCP/IP

Current Configuration

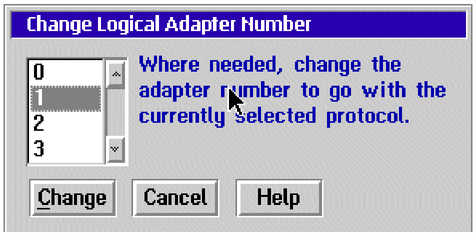
To edit driver parameters, select an item below and then select Edit.

```
IBM Compatible Token-Ring Network Adapter (IBM
        0 - IBM OS/2 NETBIOS
        0 - IBM OS/2 NETBIOS OVER TCP/IP
        0 - IBM TCP/IP
```

Select OK when complete.

Figure 49. Adapter and Protocol Configuration

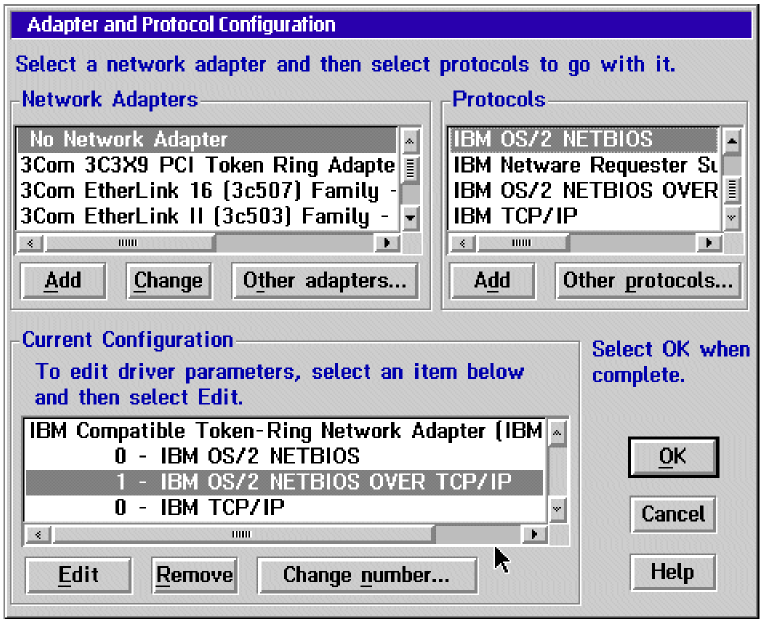
2. The current network adapter card and its protocols should be at the bottom left hand corner of the dialog box. You will need to select **IBM OS/2 NETBIOS OVER TCP/IP** on the upper right corner of the box and click **Add**.
3. You will see **IBM OS/2 NETBIOS OVER TCP/IP** included in the bottom left hand corner of the dialog box. You need to select it and click **Change number**. You will see the dialog box shown in Figure 50 on page 68.



Where needed, change the adapter number to go with the currently selected protocol.

Figure 50. Change Logical Adapter Number

4. Now, you have to change the logical adapter number. You can choose the number **1** (if it is avaiable) and click on **Change**.
5. Now, you should see the dialog box, shown in Figure 51, with a new number for your logical adapter.



Select a network adapter and then select protocols to go with it.

No Network Adapter
3Com 3C3X9 PCI Token Ring Adapte
3Com EtherLink 16 (3c507) Family -
3Com EtherLink II (3c503) Family -

IBM OS/2 NETBIOS
IBM Netware Requester Su
IBM OS/2 NETBIOS OVER
IBM TCP/IP

To edit driver parameters, select an item below and then select Edit.

```
IBM Compatible Token-Ring Network Adapter (IBM
        0 - IBM OS/2 NETBIOS
        1 - IBM OS/2 NETBIOS OVER TCP/IP
        0 - IBM TCP/IP
```

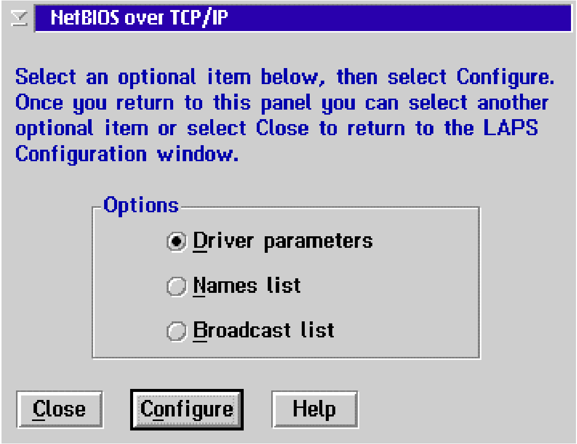
Select OK when complete.

Figure 51. New logical adapter number

4.4.1.2 Modifying the RFCNAMES file on OS/2

For each server to be accessed from the OS/2 machine, you will need to have a list of the server's NETBIOS names that maps to the server's TCP/IP address. You can use MPTS to create the list for you by doing the following:

1. Double-click on **IBM OS/2 NETBIOS OVER TCP/IP**. This should result in the panel shown in Figure 52.



NetBIOS over TCP/IP

Select an optional item below, then select Configure. Once you return to this panel you can select another optional item or select Close to return to the LAPS Configuration window.

Options

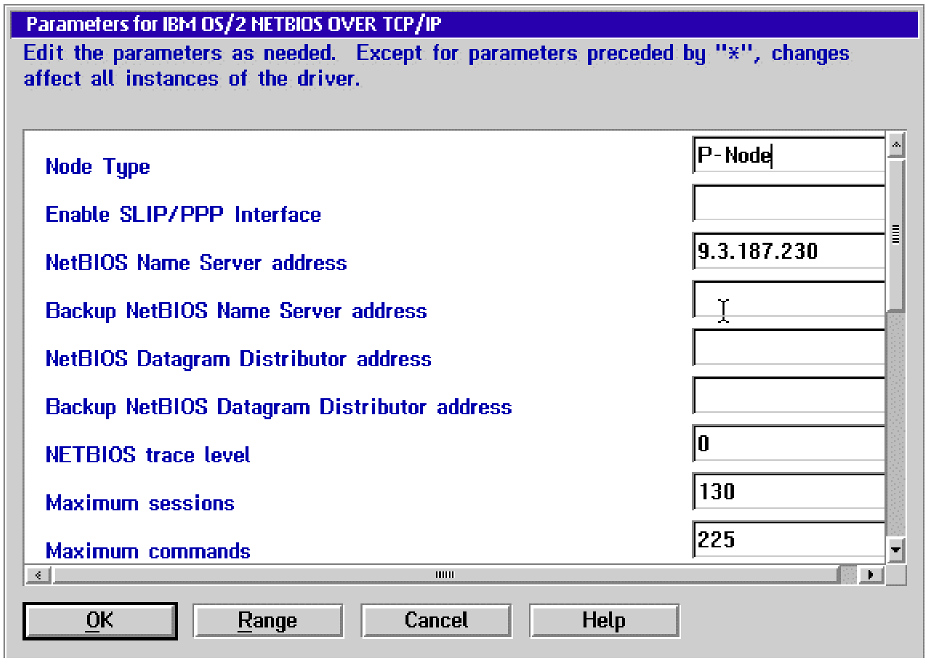
● Driver parameters

○ Names list

○ Broadcast list

Figure 52. NetBIOS over TCP/IP

2. Select **Driver parameters** and click **Configure**. You will see the dialog box shown in Figure 53 on page 70.



Parameters for IBM OS/2 NETBIOS OVER TCP/IP

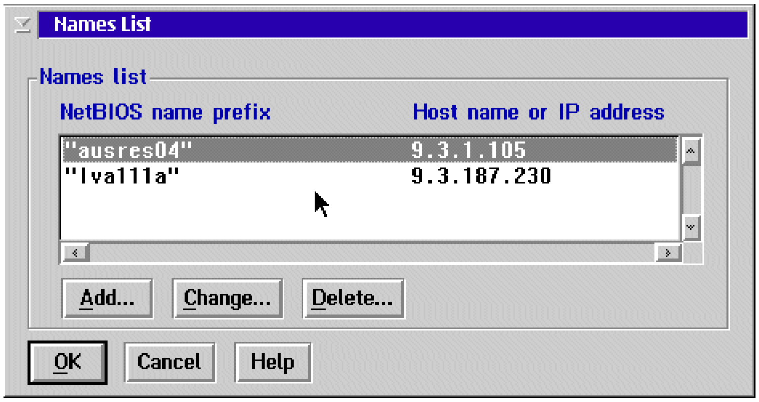
Edit the parameters as needed. Except for parameters preceded by "x", changes affect all instances of the driver.

Node Type	P-Node
Enable SLIP/PPP Interface	
NetBIOS Name Server address	9.3.187.230
Backup NetBIOS Name Server address	
NetBIOS Datagram Distributor address	
Backup NetBIOS Datagram Distributor address	
NETBIOS trace level	0
Maximum sessions	130
Maximum commands	225

Figure 53. Parameters for IBM OS/2 NETBIOS OVER TCP/IP

- Change the Node Type field to P-Node.
- In the NetBIOS Name Server address field, enter the IP Address of your name server. If you configured your Samba server with WINS support, you can enter the IP address for your Samba server here.
- Change the field Maximum number of name-ip address pairs in names file to 50.
- Click **OK**.

3. Now, select **Names list** and click **Configure**. You will see the dialog box shown in Figure 54 on page 71.



NetBIOS name prefix	Host name or IP address
"ausres04"	9.3.1.105
"lva111a"	9.3.187.230

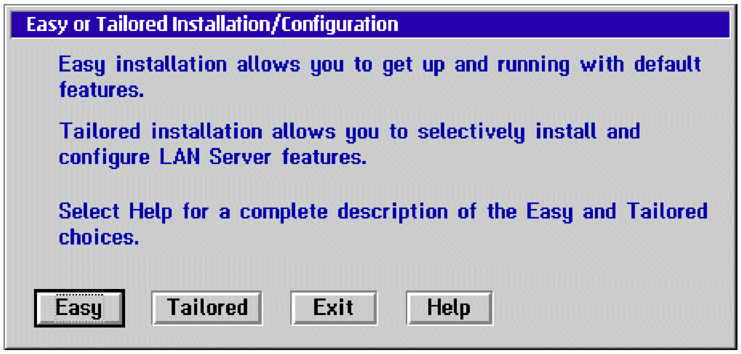
Figure 54. NetBIOS Names List

- Add the NetBIOS names and IP addresses for the SMB servers you will need to access.

4.4.1.3 Configure Lan Requester for TCPBEUI

Now that you have finished configuring the MPTS, you should configure the Lan Requester. You can follow the steps below to configure the Lan Requester:

1. Open the **LAN Services File and Print** folder.
2. Double-click **OS/2 LAN Services Installation and Configuration**.
3. You will see the IBM logo. Click **OK**.
4. You will see the dialog box show in Figure 55. Click **Easy**.



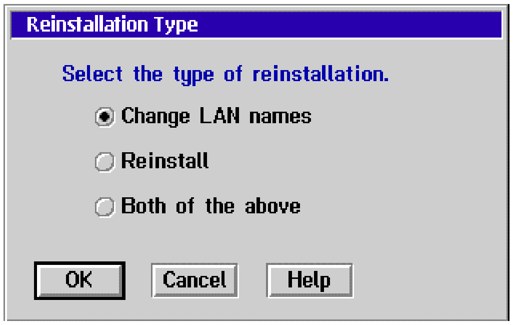
Easy installation allows you to get up and running with default features.

Tailored installation allows you to selectively install and configure LAN Server features.

Select Help for a complete description of the Easy and Tailored choices.

Figure 55. Easy or Tailored Installation/Configuration

5. You will see the dialog box shown in Figure 56. Select **Change LAN names**, and click **OK**.



Reinstallation Type

Select the type of reinstallation.

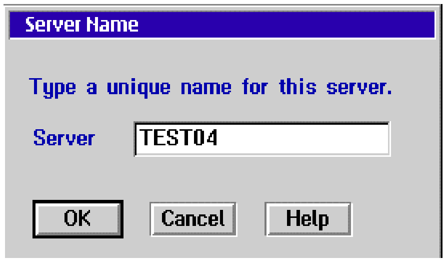
● Change LAN names

○ Reinstall

○ Both of the above

Figure 56. Reinstallation Type

6. On the next screen, you need to enter the name of the computer. Then, click **OK**. You will see the dialog box shown in Figure 57.



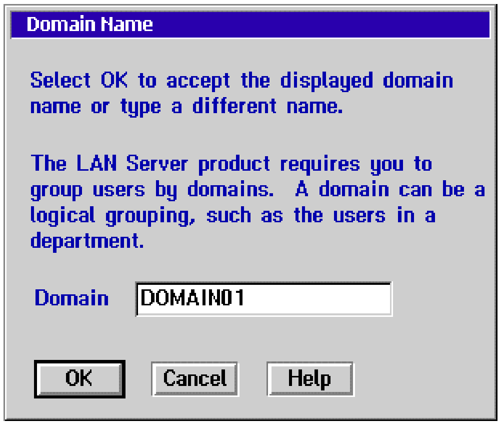
Server Name

Type a unique name for this server.

Server: TEST04

Figure 57. Server Name

7. Now, you will see the dialog box shown in Figure 58 on page 73. You have to enter the Domain name and click **OK**. In this field, you can enter the same workgroup name that you used to configure your Samba server.


Domain Name

Select OK to accept the displayed domain name or type a different name.

The LAN Server product requires you to group users by domains. A domain can be a logical grouping, such as the users in a department.

Domain DOMAIN01

Figure 58. Domain Name

8. In the Reinitialize Domain Control Database dialog box, select the **Do not reinitialize the domain control database** option and click **OK**. You will see the **LAN Software is Running** warning; this is normal. Click **OK** to continue.
9. You will see the last dialog box, Installation/Configuration Completed. Click **OK**.

4.4.1.4 Verifying the configuration

After you have configured MPTS and Lan Requester, you should check the ibmlan.ini and protocol.ini files to ensure that these files were updated with the following information below before shutting down.

IBMLAN.INI

In most cases, the ibmlan.ini file will be found in the C:\IBMLAN directory. Check for the following entries:

```
[networks]
net1 = NETBEUI$,0,LM10,102,222,14
net2 = TCPBEUI$,1,LM10,102,100,14
```

The numbers that are shown for `net1` and `net2` do not have to be identical to what is defined in your file. Lan Requester uses this information to identify which interface to use based on the protocol you are using. There will also be a line further down with the identifier, wrknets, that should look like wrknets = net1,net2.

PROTOCOL.INI

In most cases, the protocol.ini file will be found in the C:\IBMCOM directory. The file should look something like this:

```
[NETBIOS]
DriverName = netbios$
ADAPTER0 = netbeui$,0
ADAPTER1 = tcpbeui$,1

[tcpbeui_nif]
DriverName = tcpbeui$
Bindings = ,IBMTOKC_nif
NODETYPE = "P-Node"
NBNSADDR = "9.3.187.230"
OS2TRACEMASK = 0x0
SESSIONS = 130
NCBS = 225
NAMES = 21
SELECTORS = 15
USEMAXDATAGRAM = "NO"
NETBIOSTIMEOUT = 500
NETBIOSRETRIES = 2
NAMECACHE = 1000
PRELOADCACHE = "NO"
NAMESFILE = 50
DATAGRAMPACKETS = 20
PACKETS = 50
INTERFACERATE = 300
```

Shutdown and restart the system to pick up the changes.

4.4.2 Obtaining a share resource

When you want to obtain a share resource from the Samba server on an OS/2 client, there are a few helpful hints that you need to remember:

1. The user ID that is used to log on to your local LAN server must match the user ID that is used to log on to your Samba server.
2. In the `net use` command that you specify in connecting to that particular server, you will need to specify the password that you use to log on to the Samba server. If your password is the same as the one you use for a local logon, and you are logged on, you do not need to specify the password in the `net use` command.
3. You can use the `logon /l` command to do a local logon with the user ID and password that match the user ID and password in your Samba server.

This way, you do not have to specify a password when you connect to a shared resource.

In the following screens, you can see some examples of how to access a shared resource.

~~~
[<test04>-C:\]net view \\lva111a
Shared resources at \\lva111a
Samba Server

Netname      Type         Used as  Comment
`````````````````````````````````````````````````````````````````````````````
printer1     Print
test         Disk                  For testing only, please
test2        Disk                  For testing only, please
The command completed successfully.

[<test04>-C:\]net use p: \\lva111a\test
The command completed successfully.
~~~

As shown in the previous screen, you can use the `net view` command to see which resources are avaiable. Then, you can use the `net use` command to access the resource.

If you want to disconnect a shared resource, you can use the same `net view` command with the `/d` option as shown in the next screen.

~~~
[<test04>-C:\]net use

Status          Local name      Remote name
```````````````````````````````````````````````````````````````````````````````
OK              P:              \\LVA111A\TEST
The command completed successfully.

[<test04>-C:\]net use p: /d
p: was deleted successfully.

[<test04>-C:\]net use
There are no entries in the list.

[<test04>-C:\]
~~~

4.5 Using AIX as a Samba client

Sometimes, you want to access your Samba server or shares from a Windows machine using AIX. You can use the smbclient program to do this. The smbclient program is a client that can communicate with a SMB/CIFS server. If you have installed Samba using the default path, you will find it in

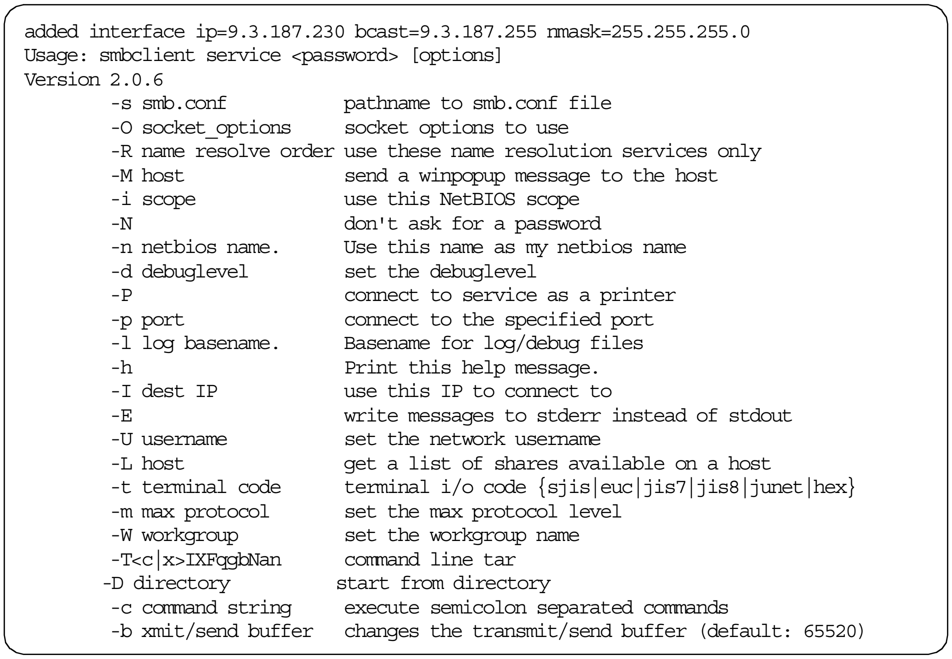
/usr/local/samba/bin. It is a good idea to include this path in your user profile. If you want to do this, you have only to add the following line in your profile:

```
PATH=$PATH:/usr/local/samba/bin
```

This client has an interface very similar to the ftp program. You can use smbclient to get files from the server to the local machine, put files from the local machine to the server, retrieve directory information from the server, and so on.

4.5.1 Accessing Windows files

Now that you have set up your profile, you can access your files in the Samba server. You can use some of the options in the command line shown in the screen below.



```
added interface ip=9.3.187.230 bcast=9.3.187.255 nmask=255.255.255.0
Usage: smbclient service <password> [options]
Version 2.0.6
        -s smb.conf           pathname to smb.conf file
        -O socket_options     socket options to use
        -R name resolve order use these name resolution services only
        -M host               send a winpopup message to the host
        -i scope              use this NetBIOS scope
        -N                    don't ask for a password
        -n netbios name.      Use this name as my netbios name
        -d debuglevel         set the debuglevel
        -P                    connect to service as a printer
        -p port               connect to the specified port
        -l log basename.      Basename for log/debug files
        -h                    Print this help message.
        -I dest IP            use this IP to connect to
        -E                    write messages to stderr instead of stdout
        -U username           set the network username
        -L host               get a list of shares available on a host
        -t terminal code      terminal i/o code {sjis|euc|jis7|jis8|junet|hex}
        -m max protocol       set the max protocol level
        -W workgroup          set the workgroup name
        -T<c|x>IXFqgbNan      command line tar
       -D directory          start from directory
        -c command string     execute semicolon separated commands
        -b xmit/send buffer   changes the transmit/send buffer (default: 65520)
```

If you want to connect to the server without specifying any other parameter, you can use the following command:

```
smbclient //<Netbios Server Name>/<Service> -U <Username>
```

> **Note**
>
> You can use \\ instead of each / if you wish. You have to use two back slashes for each slash that you want to substitute. The first back slash acts as a character escape for the second one.

You can also use some options to modify the way that you are going to connect to the server. Here are some options:

-N This option is used to suppress the normal password prompt from the client to the user. This option is very useful when you want to access a server that does not require a password to be accessed.

-p This option is used to specify the TCP/IP port that you will use when making connections. The standard TCP/IP port number for a SMB/CIFS server is 139; so, if you do not use this option, your client will try to connect to the server using the 139 port.

-I This option is used to specify the IP address of the Samba server to which you are trying to connect. This is very useful if your client is having problems using the NetBIOS name resolution.

-O This option is used when you want to specify the socket option. Here is a list of the valid options:

- SO_KEEPALIVE
- SO_REUSEADDR
- SO_BROADCAST
- TCP_NODELAY
- IPTOS_LOWDELAY
- IPTOS_THROUGHPUT
- SO_SNDBUF
- SO_SNDLOWAT
- SO_RCVLOWAT

The last four options take an integer argument.

If you are successful in connecting to the server, you will be prompted for a password. If you enter a valid password, you will see the `smbclient` prompt as shown in the following screen.

```
# smbclient //lva111a/test -U root
added interface ip=9.3.187.230 bcast=9.3.187.255 nmask=255.255.255.0
Password:
Domain=[DOMAIN01] OS=[Unix] Server=[Samba 2.0.6]
smb: \>
```

If you have problems connecting to the server, you can use the -R option before the -U option to specify which name resolution services to use when looking up the NetBIOS name. The options are:

lmhosts: This option will use the Samba lmhosts file. You can find this file in the same directory as the smb.conf file. If you have installed your Samba server using the default path, you will find this on /usr/local/samba/lib.

host: This option uses the /etc/hosts file to resolve the names. This method of name resolution depends on the operating system that you are using.

wins: Use the WINS server set up in the smb.conf file. If you do not have one specified, this method will be ignored

bcast: This option does a broadcast on the interfaces listed in the interfaces parameter in the smb.conf file. This is not a good option to choose because it depends on the target host being on a locally-connected subnet.

Now that you are accessing the Samba server, you can execute the `smbclient` commands. The following is a list of some `smbclient` commands that you can use to work with your files:

`cd` : Changes the current working directory to the specified directory. This operation will fail if the specified directory does not exists or if you do not have access.

`dir` : List the files in the current working directory. You can also use **ls** to list files.

`mkdir` : Create a new directory on the server. You can use also md.

`rmdir` : Remove a directory from the server. You can use also rd.

`lcd` : Change the local machine directory to the one specified. If the specified directory does not exist or if you do not have access to this directory, the operation will fail.

`get` : Copy the specified file from the current working directory on the server to the client. You can also use the `mget` command to copy multiple files that match a mask that you specify.

`put` : Copy the specified file from the current working directory on the local machine to the remote server. You can also use the `mput` command to copy multiple files that match a mask that you specify.

`del` : Delete all files in the current working directory that match the mask that you specify.You can also use the `rm` command.

`help` : Display a brief description of the command, if you have specified one. If not, it will display a list of all avaiable commands. You can use ? instead of using the `help` command.

`lowercase` : Toggle the option to get the files from the Samba server only in lowercase.

`prompt` : Toggle the option for filename prompts during the operation of the `mget` and `mput` commands.

`recurse` : Toggle the directory recursion for the `mget` and `mput` commands. When the toggle is on, this option will process all the directories in the source directory and will recurse into any that match the mask specified to the command.

`setmode` : This option works like the `attrib` command in DOS. If you want to change the permission of a certain file to read only, you can, for example, use setmode example.txt +r.

`exit` : This terminates the connection with the server and exits from the smbclient. You can also use quit.

4.5.2 Accessing a Windows printer

Often, you may need to print from AIX to a remote printer connected to a Windows server. The most common way to achieve this is to install the LPD service under Windows NT and print using the AIX native lpr protocol. It is also possible to configure an AIX print queue to print directly to the native Windows printer share with smbclient. This bypasses the requirement of installing extra software on the remote Windows server.

4.5.2.1 Create a printer share under Windows

Before you can remotely access a printer connected to a Windows server, it must be shared. Sharing a printer, much like sharing a file system or directory, grants network access to this device.

To install a new printer under Windows, go to the **Start Menu -> Settings -> Printers**, and select **Add Printer** or right click on an existing printer to update its properties. You will need local administration rights to install or configure a printer on the Windows server or PC.

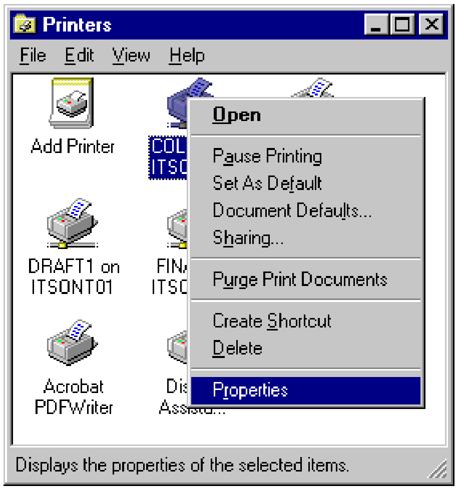
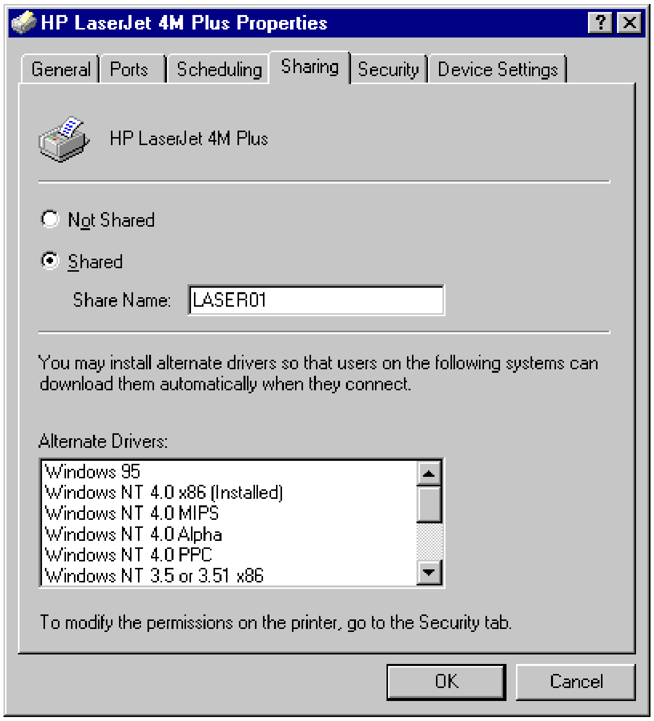


Figure 59. Select the Windows printer to configure

The next step is to define the share name for this printer. In our example, see LASER01 as shown in Figure 60 on page 81.



HP LaserJet 4M Plus

○ Not Shared

● Shared

Share Name: LASER01

You may install alternate drivers so that users on the following systems can download them automatically when they connect.

Alternate Drivers:

Windows 95
Windows NT 4.0 x86 (Installed)
Windows NT 4.0 MIPS
Windows NT 4.0 Alpha
Windows NT 4.0 PPC
Windows NT 3.5 or 3.51 x86

To modify the permissions on the printer, go to the Security tab.

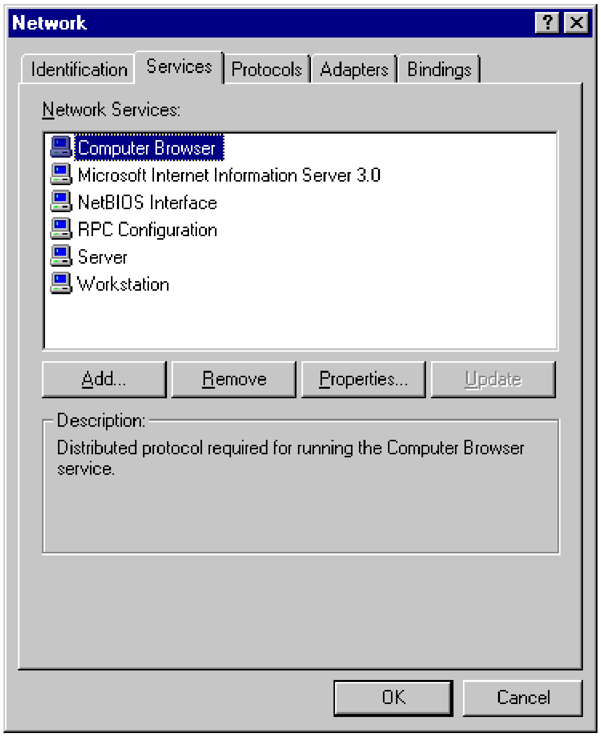
Figure 60. Sharing a Windows printer

When creating the share, you can configure the Security settings to restrict who can print to this share. If you remove Everyone from the list, you will need to specify a username and password when printing to this share via smbclient on AIX.

4.5.2.2 Print from AIX to Windows via LPD

Windows NT provides the option of installing “Microsoft TCP/IP Printing” (a recent invention from Redmond). This service allows Windows NT to accept UNIX-style LPD printer connections. Although this is not a Samba function, we will cover it here because it is very useful for AIX/Windows integration.

To install the LPD service on Windows NT, right click on **Network Neighbourhood** and select **Properties**. Then, select the **Services** tab. You should see the dialog box shown in Figure 61 on page 82.



Network Services:

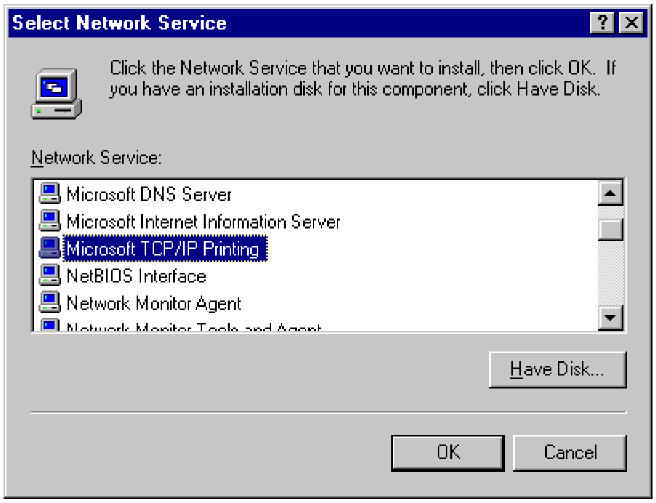
- Computer Browser
- Microsoft Internet Information Server 3.0
- NetBIOS Interface
- RPC Configuration
- Server
- Workstation

Description:

Distributed protocol required for running the Computer Browser service.

Figure 61. Network Services

Select **Add** and install the Microsoft TCP/IP Printing service as shown in Figure 62 on page 83.



Click the Network Service that you want to install, then click OK. If you have an installation disk for this component, click Have Disk.

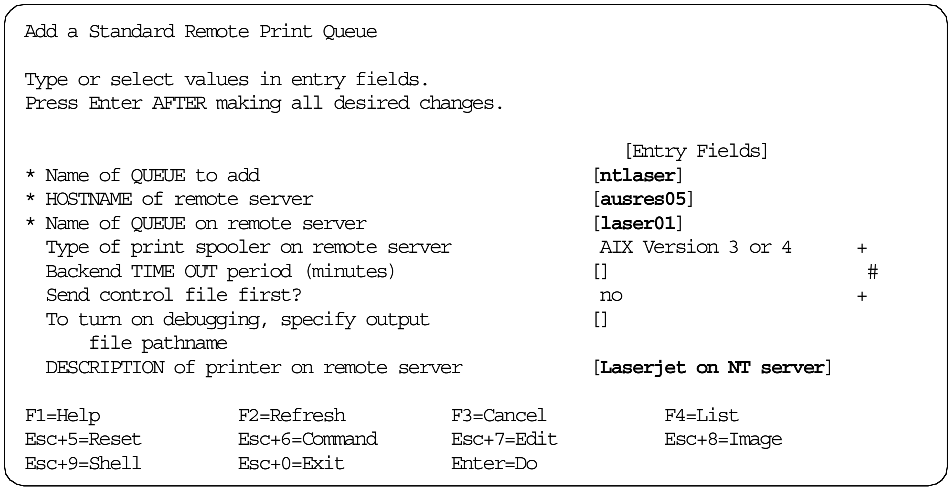
Figure 62. Select Network Service

You will need local administration rights to install this service. It will prompt you for your Windows NT installation media. After installation, you will need to reboot the Windows server.

While the Windows server is rebooting, you can configure the printer queue on AIX. Run the `smit mkpq` command and create a remote print queue.

```
lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
x                            Add a Print Queue                             x
x                                                                          x
x Move cursor to desired item and press Enter. Use arrow keys to scroll.   x
x                                                                          x
x   # ATTACHMENT TYPE      DESCRIPTION                                     x
x     local                Printer Attached to Local Host                  x
x     remote               Printer Attached to Remote Host                 x
x     xstation             Printer Attached to Xstation                    x
x     ascii                Printer Attached to ASCII Terminal              x
x     hpJetDirect          Network Printer (HP JetDirect)                  x
x     file                 File (in /dev directory)                        x
x     ibmNetPrinter        IBM Network Printer                             x
x     ibmNetColor          IBM Network Color Printer                       x
x     other                User Defined Backend                            x
x                                                                          x
x F1=Help                 F2=Refresh              F3=Cancel                x
x Esc+8=Image             Esc+0=Exit              Enter=Do                 x
x /=Find                  n=Find Next                                      x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

Select **remote - Printer Attached to a Remote Host**, and then select **Standard processing**.



```
Add a Standard Remote Print Queue

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                       [Entry Fields]
* Name of QUEUE to add                              [ntlaser]
* HOSTNAME of remote server                         [ausres05]
* Name of QUEUE on remote server                    [laser01]
  Type of print spooler on remote server             AIX Version 3 or 4      +
  Backend TIME OUT period (minutes)                 []                        #
  Send control file first?                           no                      +
  To turn on debugging, specify output              []
      file pathname
  DESCRIPTION of printer on remote server           [Laserjet on NT server]

F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

You should now be able to print to this remote Windows/LPD printer share exactly as you would to a remote UNIX printer.

The remote Windows server should pass through the AIX print output, without translation, directly to the printer.

4.5.2.3 Printing from AIX to Windows with smbclient

It is possible to print directly from AIX to an existing Windows shared printer without installing the LPD service on the Windows server.

You need to configure an AIX print queue to send its output to a user-defined backend script. The script can then call smbclient to send the output, by way of the SMB protocol, directly to an existing Windows printer share.

Since the backend script is handcrafted to suit our needs, it can be very flexible. We can reformat the output to better suit a particular brand of printer, correct carriage return/line feed issues, and so on. In fact, the backend script can be designed to perform a number of non-printing functions with its input. For example, a user can print postscript output from their PC application, which is then converted to a gif image for display on a Web page.

The following is an example script that simply converts carriage returns to carriage return/line feed pairs and forwands its input directly to a remote

Windows printer. It contains an optional line to translate postscript input to something suitable for a non-postscript printer.

```
#!/bin/sh -f

WINDOWS_HOST=itsont01
PRINTER_SHARE=draft1

# Send all output to /dev/null
exec >/dev/null 2>&1

# Optional - convert postscript input for non-postscript printer
#gs -sDEVICE=<driver> -q -sOutputFile=/tmp/printer.$$.tmp $1

# Fix "stair-stepping" on some printers (CR to CR/LF translation)
sed 's/$/^M/;$ s/$/^Z/' $1 > /tmp/print.$$.tmp

# Send output to the remote Windows printer
# This may require "-Uusername%password" depending on Windows printer share
smbclient //$WINDOWS_HOST/$PRINTER_SHARE -P -c "put /tmp/print.$$.tmp"

# Remove temporary file
rm /tmp/print.$$.tmp

~
~
~
"sample_script.sh" 21 lines, 577 characters
```

The script can be written in any language that AIX can process. You may want to consider enhancing this script to better suit your environment. For example:

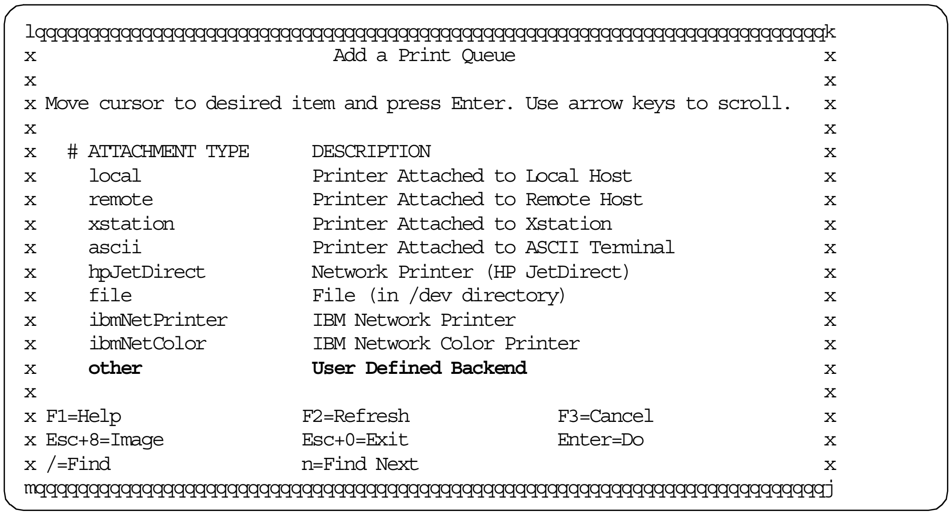
- Perform CR to CR/LF translation
- Prepend some printer configuration to the data
- Translate postscript or graphical input into something suitable for your printer

You can test this script at the command line by passing it a small text file:

```
sample_script.sh /usr/local/samba/lib/smb.conf
```

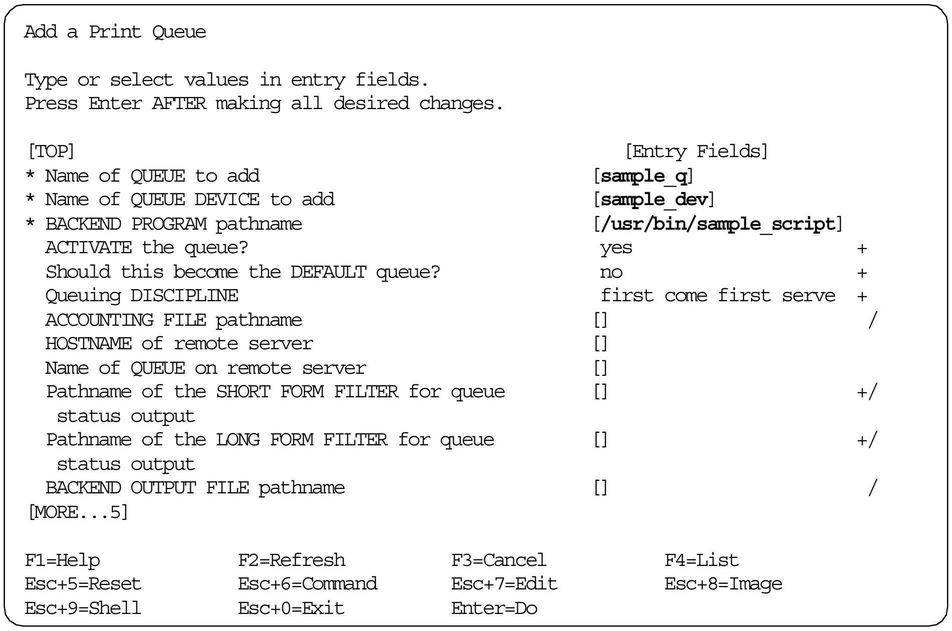
Next, we need to configure a new print queue to call the backend script. Run the following command:

```
smitty mkpq
```



```
lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
x                            Add a Print Queue                             x
x                                                                          x
x Move cursor to desired item and press Enter. Use arrow keys to scroll.   x
x                                                                          x
x   # ATTACHMENT TYPE      DESCRIPTION                                     x
x     local                Printer Attached to Local Host                  x
x     remote               Printer Attached to Remote Host                 x
x     xstation             Printer Attached to Xstation                    x
x     ascii                Printer Attached to ASCII Terminal              x
x     hpJetDirect          Network Printer (HP JetDirect)                  x
x     file                 File (in /dev directory)                        x
x     ibmNetPrinter        IBM Network Printer                             x
x     ibmNetColor          IBM Network Color Printer                       x
x     other                User Defined Backend                            x
x                                                                          x
x F1=Help                 F2=Refresh             F3=Cancel                 x
x Esc+8=Image             Esc+0=Exit             Enter=Do                  x
x /=Find                  n=Find Next                                      x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

Select **other - User Defined Backend**



```
Add a Print Queue

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP]                                                   [Entry Fields]
* Name of QUEUE to add                               [sample_q]
* Name of QUEUE DEVICE to add                        [sample_dev]
* BACKEND PROGRAM pathname                           [/usr/bin/sample_script]
  ACTIVATE the queue?                                 yes                   +
  Should this become the DEFAULT queue?               no                    +
  Queuing DISCIPLINE                                  first come first serve +
  ACCOUNTING FILE pathname                           []                      /
  HOSTNAME of remote server                          []
  Name of QUEUE on remote server                     []
  Pathname of the SHORT FORM FILTER for queue        []                     +/
   status output
  Pathname of the LONG FORM FILTER for queue         []                     +/
   status output
  BACKEND OUTPUT FILE pathname                       []                      /
[MORE...5]

F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

Enter the name of the new AIX printer queue, the new queue device, and the backend script to process the output.

You can now check the status of the remote SMB printer with the following command:

```
lpr -Psample_q /usr/local/samba/lib/smb.conf
```

You should now be able to print to this remote Windows printer share exactly as you would to a remote UNIX printer.

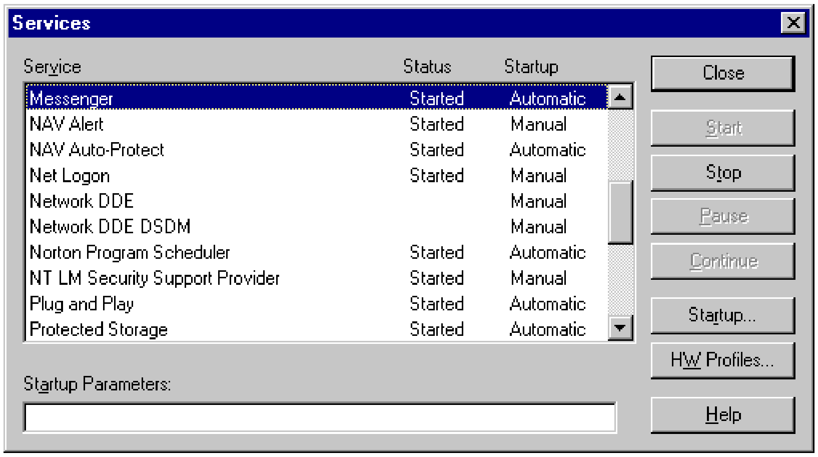
4.5.3 Messaging

We can use the smbclient program to send and receive Windows pop-up messages. In this section, we will describe what you need to do to use smbclient to send and receive messages.

4.5.3.1 Windows configuration

If you are using Windows 95/98, you need to have the Windows pop-up program running on the PC to receive the messages. This program is included with the standard Client for Microsoft Networks software. If your Windows pop-up is not running, you can start by executing c:\windows\winpopup.exe..

If you are running Windows NT or Windows 2000, you need to check if the Messenger service is running. In Windows NT, click on **Start -> Settings -> Control Panel** and double-click on the **Services** icon. You should see the dialog box shown in Figure 63.



Services

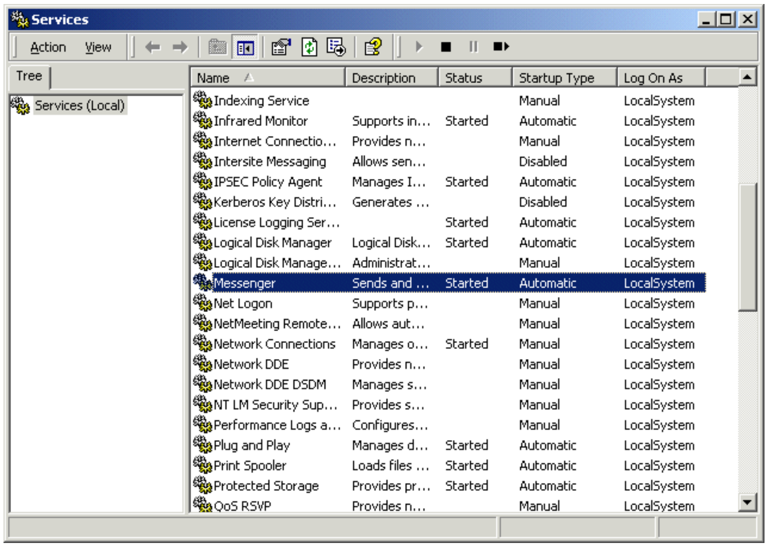
Service	Status	Startup
Messenger	Started	Automatic
NAV Alert	Started	Manual
NAV Auto-Protect	Started	Automatic
Net Logon	Started	Manual
Network DDE		Manual
Network DDE DSDM		Manual
Norton Program Scheduler	Started	Automatic
NT LM Security Support Provider	Started	Manual
Plug and Play	Started	Automatic
Protected Storage	Started	Automatic

Startup Parameters:

Figure 63. Services - Windows NT

If the Messenger service is stopped, you have to start it. You only have to select the service and click the **Start** button.

In Windows 2000, click on **Start -> Programs -> Administrative Tools -> Services**. You should see the dialog box shown in Figure 64.



Name	Description	Status	Startup Type	Log On As
Indexing Service			Manual	LocalSystem
Infrared Monitor	Supports in...	Started	Automatic	LocalSystem
Internet Connectio...	Provides n...		Manual	LocalSystem
Intersite Messaging	Allows sen...		Disabled	LocalSystem
IPSEC Policy Agent	Manages I...	Started	Automatic	LocalSystem
Kerberos Key Distri...	Generates ...		Disabled	LocalSystem
License Logging Ser...		Started	Automatic	LocalSystem
Logical Disk Manager	Logical Disk...	Started	Automatic	LocalSystem
Logical Disk Manage...	Administrat...		Manual	LocalSystem
Messenger	Sends and ...	Started	Automatic	LocalSystem
Net Logon	Supports p...		Manual	LocalSystem
NetMeeting Remote...	Allows aut...		Manual	LocalSystem
Network Connections	Manages o...	Started	Manual	LocalSystem
Network DDE	Provides n...		Manual	LocalSystem
Network DDE DSDM	Manages s...		Manual	LocalSystem
NT LM Security Sup...	Provides s...		Manual	LocalSystem
Performance Logs a...	Configures...		Manual	LocalSystem
Plug and Play	Manages d...	Started	Automatic	LocalSystem
Print Spooler	Loads files ...	Started	Automatic	LocalSystem
Protected Storage	Provides pr...	Started	Automatic	LocalSystem
QoS RSVP	Provides n...		Manual	LocalSystem

Figure 64. Services dialog box - Windows 2000

If the Messenger service is stopped, you have to start it. You have to select and right-click the **Messenger** icon, and then click **Start**.

4.5.3.2 Using the smbclient to send and receive messages

You should use the `-M` option followed by the computer name of the recipient to send messages using the Winpopup protocol. You can see an example in the following screen:

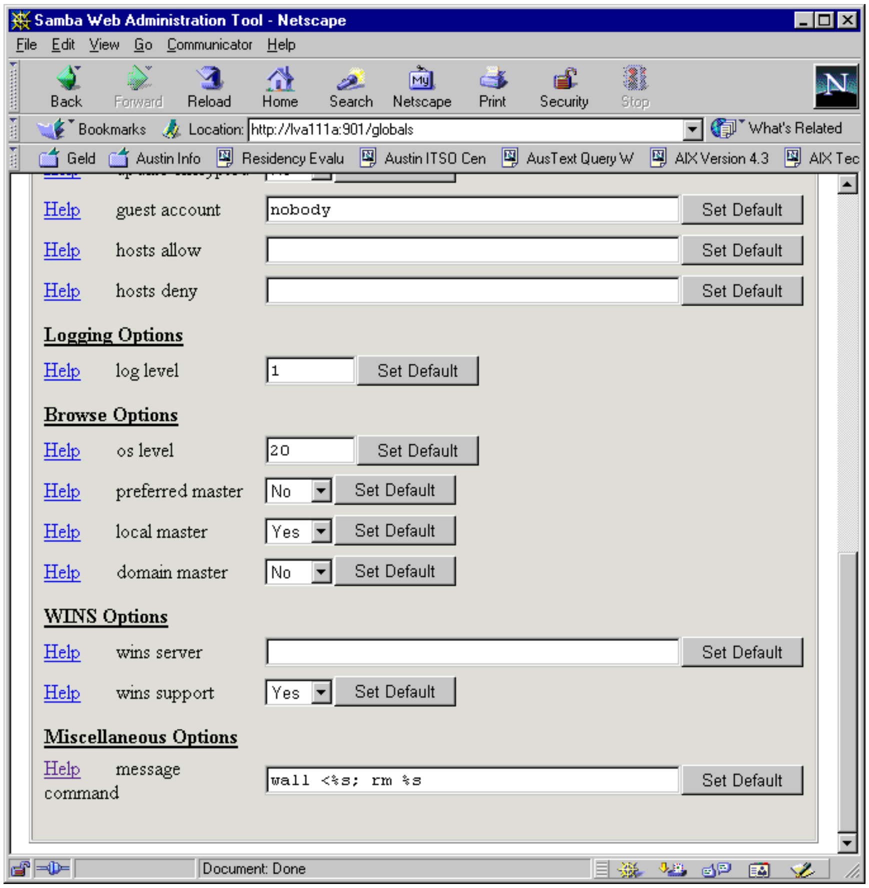
```
root@lva111a[/] smbclient -M ausres04
added interface ip=9.3.187.230 bcast=9.3.187.255 nmask=255.255.255.0
Connected. Type your message, ending it with a Control-D
Hello!
sent 8 bytes
root@lva111a[/]
```

You can also redirect the output of a command to `smbclient`.:

```
cat message.txt | smbclient -M ausres04
```

This command will redirect the output of the `cat` command to `smbclient`; so, the recipient machine will receive a message with the contents of the message.txt file. This can be useful if you want to automate some tasks.

To receive a Windows pop-up message, you need to configure your smb.conf file. You can do this using SWAT or by editing the file. If you want to configure the option using SWAT, you should first log on to SWAT, and then click on **Globals** and go to the bottom of the page as shown in Figure 65.


Samba Web Administration Tool - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://lva111a:901/globals
What's Related
Geld Austin Info Residency Evalu Austin ITSO Cen AusText Query W AIX Version 4.3 AIX Tec
Document: Done

Help guest account nobody Set Default

Help hosts allow Set Default

Help hosts deny Set Default

Logging Options

Help log level 1 Set Default

Browse Options

Help os level 20 Set Default

Help preferred master No Set Default

Help local master Yes Set Default

Help domain master No Set Default

WINS Options

Help wins server Set Default

Help wins support Yes Set Default

Miscellaneous Options

Help message command `wall <%s; rm %s` Set Default

Figure 65. Miscellaneous Options

In Miscellaneous Options, you will find the message command field. In this field, you should enter the command that you want to execute when a message arrives. For example, if you want to broadcast a message for all users when a message arrives, you can use the following command:

```
wall <%s; rm %s
```

The variable, `%s`, has the name of the file that contains the message. This way, every message that arrives on the server will be shown using a broadcast for all the users. You can use more variables to build your commands. The following is a list with other variables that you can use:

%t The destination to which the message was sent (probably, the server name).

%f Who the message is from.

If you want to configure this editing the smb.conf, you need to add the following line on the global section:

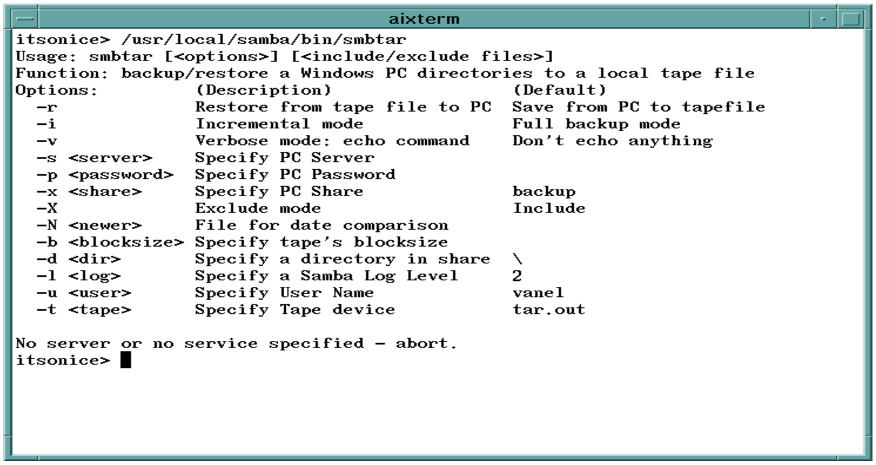
```
message command = wall <%s; rm %s
```

The following screen shows an example of an smb.conf file with this configuration:

```
# Global parameters
[global]
        workgroup = DOMAIN01
        netbios name = LVA111A
        encrypt passwords = Yes
        wins support = Yes
        message command = wall <%s; rm %s
```

4.5.4 Using Samba to back up a client

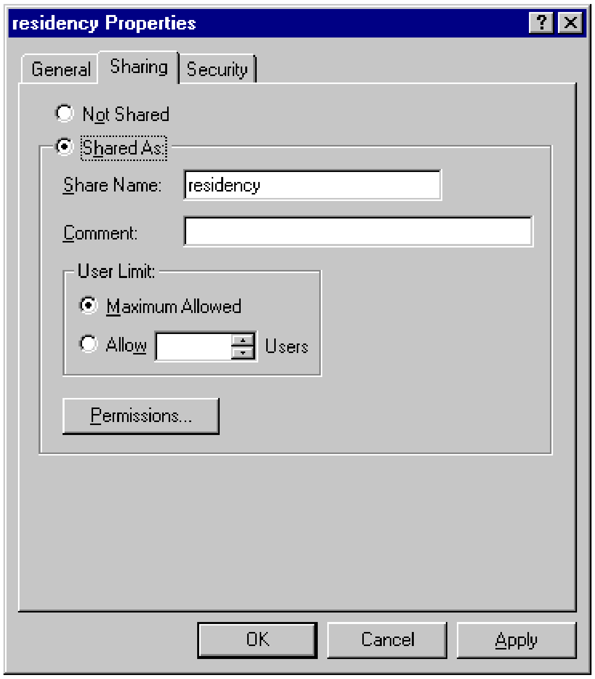
Samba offers a simple solution to back up the data you have on your Windows NT client. The `smbtar` command is part of the standard distribution and resides in the default /usr/local/samba/bin directory. It uses the standard tar format to back up the data to a file or a tape attached to the server.



```
itsonice> /usr/local/samba/bin/smbtar
Usage: smbtar [<options>] [<include/exclude files>]
Function: backup/restore a Windows PC directories to a local tape file
Options:         (Description)                 (Default)
  -r             Restore from tape file to PC  Save from PC to tapefile
  -i             Incremental mode              Full backup mode
  -v             Verbose mode: echo command    Don't echo anything
  -s <server>    Specify PC Server
  -p <password>  Specify PC Password
  -x <share>     Specify PC Share              backup
  -X             Exclude mode                  Include
  -N <newer>     File for date comparison
  -b <blocksize> Specify tape's blocksize
  -d <dir>       Specify a directory in share  \
  -l <log>       Specify a Samba Log Level     2
  -u <user>      Specify User Name             vanel
  -t <tape>      Specify Tape device           tar.out

No server or no service specified - abort.
itsonice> █
```

Figure 66. 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** tab. You should get the panel shown in Figure 67 on page 92. You must enter the name you want to give to this shared resource; the default is the name of the directory. Click the **OK** button; your directory is now accessible from the network.



○ Not Shared

● Shared As:

Share Name: residency

Comment:

User Limit:

● Maximum Allowed

○ Allow Users

Figure 67. Sharing a directory

To check that this resource is available, use the `smbclient` command. The example in the following screen 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. 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 to automate the backup, for example, at night.

The following example shows the result of the `smbtar` command.

```
# 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
```

You also can use others parameters:

-N filename: This option only backs up files that are newer than the file you specified in the filename. This option can be very useful if you want to implement an incremental backup to a log file.

-i: This option is used if you want to perform an incremental backup. This way, the files are only backed up if they have the archive bit set. You should know that the archive bit is reset after the file is read.

Once your backup is finished, you can verify the result by using the standard UNIX `tar` command as shown in the following screen:

```
# 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
#
```

If you want to use a tape attached to the server instead of a file, you first need to check if there is a tape drive avaiable. You can check this using the `lsdev` command as shown in the following screen:

```
root@lva111a[/] lsdev -Cc tape
rmt0 Available 04-B0-00-0,0 4.0 GB 4mm Tape Drive
```

Now, you can insert a tape in the tape drive and start the backup. To start it, you can use the same command that you used to back up a file, but you need to change the -t parameter. Instead of the name of the file, you need to use the tape device that you are going to use. An example is shown in the following screen:

```
root@lva111a[/] smbtar -v lv3010j -u administrator-x residency -t /dev/rmt0
server    is lv3010j
share     is residency\
tar args  is
tape      is /dev/rmt0
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=[DOMAIN01] OS=[Windows NT 4.0] Server=[NT LAN Manager 4.0]
   1152512 (  179.1 kb/s) \ad302.exe
   3578900 (  409.7 kb/s) \sg245139.pdf
   4443893 (  384.9 kb/s) \sg245129.pdf
   4049349 (  397.6 kb/s) \sg242014.pdf
   5760288 (  262.7 kb/s) \ar405eng.exe
   1229436 (  442.1 kb/s) \4_3_3_guide.pdf
tar: dumped 6 files and directories
Total bytes written: 20216320
```

To check the results, you can use the `tar` command again. The command is the same that you used above to check the backup using a file. You only have to use the tape device instead of the name of the file. You can see the command in the following screen:

```
root@lva111a[/] tar -tvf /dev/rmt0
-rw-r--r--   0 0  1152512 Jun 28 13:54:18 1999 ./ad302.exe
-rw-r--r--   0 0  3578900 Oct 20 13:15:26 1999 ./sg245139.pdf
-rw-r--r--   0 0  4443893 Oct 20 13:25:02 1999 ./sg245129.pdf
-rw-r--r--   0 0  4049349 Oct 21 17:08:50 1999 ./sg242014.pdf
-rw-r--r--   0 0  5760288 Feb 16 16:11:06 2000 ./ar405eng.exe
-rw-r--r--   0 0  1229436 Oct 19 13:40:52 1999 ./4_3_3_guide.pdf
root@lva111a[/]
```

Restoring the files to your client is just as easy. To do so, use the -r option, as shown in the following screen:

```
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
#
```

To restore using the tape that you have attached, you can use the same command, and only modify the `-t` parameter to the tape device that you are using.

Chapter 5. Advanced configuration

One of the best Samba features is its huge array of configuration and tuning parameters. With the wide variety of clients, each with their own idiosyncrasies, SMB networking rapidly becomes quite complex. This presents a challenge for the new administrator, who needs to know what to configure to suit each environment. Fortunately, most parameters can be left with their default settings and only changed on an as-needed basis.

In this chapter, we explain the mysteries of password synchronization, how to join an existing Windows NT Domain, use Samba as a Domain Controller, deliver roaming user profiles, provide a netlogon service, and other miscellaneous options.

5.1 Security options

The SMB protocol supports two modes of access control: Share-level and user-level security. Samba implements both modes and offers two additional modes for passthrough authentication to a remote password server or domain controller.

Samba can be configured to respond to multiple NetBIOS names, in effect, running multiple servers with different resources and security settings. Also, the smb.conf file can import client-specific configuration information to further customize access control.

5.1.1 Security-level parameter

The security-level setting is one of the most important parameters when configuring Samba. It controls how the Samba server reports its security requirements to the connecting client and how the client will respond to the authentication challenge. The security-level is a global setting and applies to all shares on a Samba server.

The following parameters in the global section of the smb.conf file control the server's security-level.

5.1.1.1 Share-level security

This was Samba default security level prior to Version 2.0.0. It only requires the client to present a valid password prior to gaining access to a shared resource; it does not expect a username. Anyone, regardless of username, can access the shared resource if they know the correct password. Different passwords can grant different levels of access, for example, one password for read-only access, another for read-write, and so on.

Samba will determine which AIX username to use depending on whether a username was presented with the connection, the client's NetBIOS name, guest access parameter, previous connections, service name, and user list. It can sometimes be confusing to determine which AIX username will be used in share-level security.

Share-level security can be useful when you want to set up an unrestricted printer server or when your PC client usernames do not match your AIX usernames. If a share is guest-only, the user is immediately granted access without the need to present a password.

parameter: `security = share`

5.1.1.2 User-level security

This is the default SMB authentication method used by Samba. It requires the client to present a valid username and password when connecting to the server. The name of the share to which to connect is not sent until access is granted by the server.

You should use the valid users parameter to restrict which users can connect to any particular share. Guest-only shares do not work in user-level security without allowing the server to map unknown users into the *guest account*.

User-level security is the preferred mode of security in Samba. It matches the default security mode of Windows NT and allows clients to provide either encrypted or unencrypted passwords.

parameter: `security = user`

5.1.1.3 Server-level security

Samba 2.0.0 introduced a passthrough authentication capability to a remote SMB password server. This could either be another Samba server or a Windows server. As far as the client is aware, the server is in user-level security mode.

The same restrictions present for user-level security also apply to server-level security. Access to your Samba server is now dependant on the network availability of the password server. The password server parameter accepts the NetBIOS name, not the DNS name of one or more SMB servers. Ensure that your server can reliably contact the PDC and BDCs when using server-level security.

Server-level security is useful when your user population does not need interactive AIX accounts. It allows you to control Samba access based on valid Domain username and password combinations.

parameters: `security = server`

```
password server = <remote server>
```

5.1.1.4 Domain-level security

Samba 2.0.X introduced the ability to join an existing Windows NT Domain as a member server, and to trust the Primary Domain Controller with the authentication process. As far as the client is aware, the server is in user-level security.

This mode will only function correctly after the Samba server has been made a member of the Domain serviced by the PDC. Otherwise, the same restrictions present for user-level security also apply to domain-level security. Access to your Samba server is now dependant on the network availability of the password server. The password server parameter accepts the NetBIOS name, not the DNS name of one or more SMB servers. Ensure that your server can reliably contact the PDC and BDCs when using server-level security.

Domain-level security is useful when your user population does not need interactive AIX accounts. It allows you to control Samba access based on valid Domain username and password combinations.

parameters: `security = domain`

```
          password server = <remote server>
```

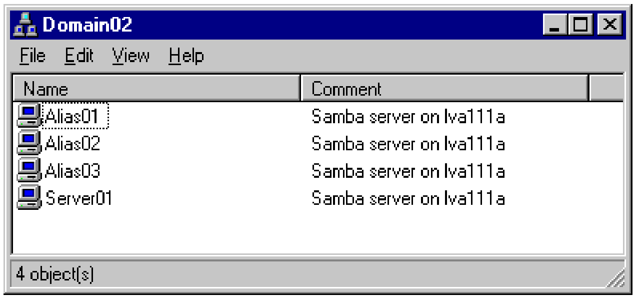
Note

Regardless of the security-level chosen, Samba *always* requires a corresponding AIX account be available on the local server. This allows the smbd daemon, originally running as root, to *su* to the connecting user’s account in order to keep track of file system access permissions and file ownership.

5.1.1.5 NetBIOS aliases

It is possible to use Samba in a *hybrid mode* where it offers both user and share level security under different NetBIOS aliases. This could be useful when consolidating multiple smaller servers onto a larger server or when serving resources with different security requirements. For example, configure a file server in user-level security and a printer server in share-level security with guest access turned on.

First, configure Samba as is usually done for a single server, and then add the netbios aliases parameter. This will cause Samba to announce the availability of the new virtual servers making them appear in the client browse list. If a machine is acting as a browse server or logon server, only the primary name of the machine will be advertised with these capabilities.



Name	Comment
Alias01	Samba server on lva111a
Alias02	Samba server on lva111a
Alias03	Samba server on lva111a
Server01	Samba server on lva111a

4 object(s)

Figure 68. Client browse list showing virtual Samba servers

You can use the include parameter to load a customized smb.conf file for each virtual server. The `%L` variable can be used to substitute for the name of the server to which the client is connecting. You could even configure each virtual server to run in a separate Domain.

The primary smb.conf file might look something like this:

```
[global]
   workgroup = DOMAIN02
   netbios name = SERVER01
   server string = Samba server on %h

   netbios aliases = ALIAS01 ALIAS02 ALIAS03
   include = /usr/local/samba/lib/smb.conf.%L

   security = user
   encrypt passwords = Yes

[test]
   comment = For testing only, please
   path = /usr/samba/test
   read only = No
   guest ok = Yes
```

And the smb.conf.alias01 file might look totally different, like this:

```
[global]
   workgroup = DOMAIN02
   netbios name = ALIAS01
   server string = Samba server on %h

   encrypt passwords = Yes
   secutiry = share

[laser01]
   comment = Draft laser printer
   path = /tmp
   guest ok = Yes
   print ok = Yes
   read only = Yes
```

5.1.1.6 Multiple smb.conf files

The include parameter used in the previous section can also be used to customize the smb.conf file for particular users and client types. This can be useful if some of your client platforms have conflicting security requirements.

The include parameter can be used in the global section and in individual shares. All the standard variable substitutions described in Section 3.1.2, “Parameters” on page 16, except %u, %P, and %S, can be used to customize the configuration. Parameters set in the include file will overwrite any duplicates in the main smb.conf

```
[global]
   workgroup = DOMAIN02
   netbios name = SERVER01
   server string = Samba server on %h

   netbios aliases = ALIAS01 ALIAS02 ALIAS03
   include = /usr/local/samba/lib/smb.conf.%L

   security = user
   encrypt passwords = Yes

[test]
   comment = For testing only, please
   path = /usr/samba/test
   include = /usr/local/samba/lib/test.conf.%a
   read only = No
   guest ok = Yes
```

You should not use SWAT after you have added the `include` parameter since SWAT cannot parse this parameter and will truncate the %L variable.

5.2 Usernames and Passwords

UNIX and Windows approach security with many different assumptions. While AIX is only aware of local accounts (UID), Windows systems have both local and Domain accounts (SID). Each system implements different password hashing algorithms and has different rules on what constitutes a valid username and password.

5.2.1 AIX and Windows user accounts

Differences between AIX and Windows usernames and passwords will sometimes cause difficulty when accessing a Samba server. It is quite possible to create a username on one system that cannot be created on the other. Simply synchronizing account and password data between the two systems can sometimes be a challenge.

AIX and Windows have different rules on which characters are valid in a username.

Table 5. Restrictions on AIX and Windows usernames

	AIX	Windows
Invalid characters	: Colon / Forward slash \ Back slash = Equal sign , Comma ? Question mark " Double quote # Pound sign ' Single quote ` Back quote ‘ ‘ Space	: Colon ; Semi-colon / Forward slash \ Back slash = Equals sign , Comma ? Question mark [Left square bracket] Right square bracket | Vertical bar + Plus sign * Asterix < Less than sign > Greater than sign
Invalid usernames	ALL, default	
Other limitations	Must not start with a - (dash), + (plus sign), @ (at sign), or ~ (tilde)	Must include more than only periods (.) and spaces

AIX usernames are case-sensitive and limited to no more than eight characters in length. They can include double-byte characters. AIX passwords are case-sensitive and can be arbitrarily long, although, only the first eight characters are considered distinct, with extra characters ignored during the logon process.

The various Windows clients each have their differing limitations on username and password syntax. Most Windows systems allow usernames of up to 20 characters, although, Windows 98 allows up to 128 characters. Windows usernames are not case-sensitive. Older Windows clients only allow short, case-independent passwords and often uppercase them during authentication. More recent Windows clients use case-sensitive passwords of up to 14 characters in length.

The best cure for these incompatibilities is forward planning when designing your user account policies, but Samba also offers some mechanisms to map between the AIX and Windows standards.

5.2.2 Username mapping

It may happen that your users' names on their client stations are not the ones to which they want to connect 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 need to perform the following steps:

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 on to an NT system with the user *admin* or *administrator* can access the Samba server and provide the *root* password for authentication; the translation between the pairs admin/password and root/password will be done automatically by Samba.

This can also be used to allow clients with long NetBIOS names to join a Domain that uses Samba TNG on AIX as the PDC. The eight-character AIX username limitation normally stops clients with long NetBIOS names from joining a Domain that uses Samba on AIX as the PDC. You can create valid AIX accounts for these systems and map them to their longer NetBIOS names. Refer to Section 5.4, “Using Samba as a primary domain controller (PDC)” on page 112.

5.2.3 Encrypted vs. unencrypted passwords

When a client attempts to connect to a shared resource on a SMB server, it sends the username and password across the network for authentication by the remote server. This creates the possibility that someone will eavesdrop on the session authentication and obtain your network password. Once someone else has your password they can effectively impersonate you on the network and access any network resources to which you legitimately have access.

Older versions of SMB clients (Windows for Workgroups, Windows 95 and Windows NT pre service pack 3) send their passwords across the network as clear, unencrypted, text. This allows anyone with modest technical skill to collect your password simply by running a packet sniffer on the same network segment. Recent versions of SMB clients (Windows 98 and NT post service pack 3) encrypt your password prior to sending it across the network.

The Samba distribution comes with instructions and registry patches to force recent clients to use unencrypted passwords. Refer to Chapter 4, “Client configuration” on page 29 for details on how to configure password encryption on the clients.

Refer to the ENCRYPTION.txt file included with the Samba documentation for more details on password encryption with Samba.

5.2.3.1 Configuring Samba

By default, Samba is configured to use unencrypted passwords and can only accept connections from clients that also use unencrypted passwords. Later, if you chose to configure Samba to use encrypted passwords (this is recommended), it will no longer be able to accept connections from clients using unencrypted passwords.

To assist with migration from unencrypted to encrypted client passwords, Samba offers a mechanism to automatically update client passwords as they connect. Refer to Section 5.2.3.3, “Migration to encrypted passwords” on page 106, for details.

You can configure Samba to only accept connections from clients using encrypted passwords by adding the following parameter to the [global] section of the smb.conf file:

```
[global]
```

```
encrypted passwords = yes
```

Before you can connect from clients using encrypted passwords, you will need to create a smbpasswd file to contain the encrypted client passwords. Refer to Section 5.2.3.2, “Creating a smbpasswd file” on page 105.

5.2.3.2 Creating a smbpasswd file

Because of the different password hashing algorithms used by AIX and the SMB challenge/response protocol, Samba cannot authenticate an encrypted Windows password against the encrypted AIX password. A separate file, called smbpasswd, is required to store the client’s encrypted passwords.

To create and maintain the smbpasswd file, use the command of the same name: `smbpasswd`. The `smbpasswd` command can also be used to change SMB passwords on remote systems (including a PDC), join the Samba server to a Domain, and enable/disable Samba users.

The smbpasswd file has the following structure:

```
username:uid:<LM passwd hash>:<NT passwd hash>:[U]:LCT-XXXXXXXX:
```

The smbpasswd file contains the Samba users’ passwords in both LAN Manager (LM) and NT style hashes. The 11 characters between the square brackets are the account flags; they can contain any of the following, in any order, followed by spaces:

U Indicates a standard user account

W Indicates a Workstation trust account.

N This account has no password

D This account is disabled

The value after LCT (Last Change Time) is the time of the last password change, in seconds since 1970.

This is an important security file and should be treated much like a shadow password file. By default, it is stored in the /usr/local/samba/private directory and is readable only by root.

- To add an individual user to the smbpasswd file, enter the following command:

  ```
  smbpasswd -a <username>
  ```

  After the users have been added to the smbpasswd file, they can manually change their own Samba password with the same command:

  ```
  smbpasswd <username>
  ```

The SWAT interface also allows an administrator to add and remove users and change their passwords.

Samba comes with a script, called mksmbpasswd.sh (located in the distribution source/scripts directory), to help populate the smbpasswd file with the existing usernames defined on your system. Note that, just as Samba cannot compare the encrypted Windows password with the encrypted AIX password, this script can only provide the usernames and not the encrypted passwords of your users. You will need to either get your users to manually update their Samba passwords or migrate their passwords gradually using the *update encrypted* parameter. Refer to Section 5.2.3.3, “Migration to encrypted passwords”, on this page, for more details.

- To import all user account names from a non-NIS system, enter:

  ```
  cat /etc/passwd | mksmbpasswd.sh > /usr/local/samba/private/smbpasswd
  ```

  or, on a system using NIS, enter:

  ```
  ypcat passwd | mksmbpasswd.sh > /usr/local/samba/private/smbpasswd
  ```

  In both cases, the new smbpasswd file will have invalid passwords and will need to be updated before your users can connect successfully.

- If you want to change the default path to the smbpasswd file, edit the smb.conf file as shown here:

  ```
  smb passwd file = /usr/local/samba/private/smbpasswd
  ```

- You will need to modify the smb.conf file to use encrypted passwords before your system will use the smbpasswd file for authentication. For example:

  ```
  encrypt passwords = yes
  ```

Once the smbpasswd file has been created, your users can maintain their own Samba passwords with the smbpasswd command.

Storing the user’s password in two locations provides the opportunity for the AIX and Samba passwords to differ over time. Although this will not prevent your users from accessing either AIX or Samba, it may require them to remember a separate password for each system.

5.2.3.3 Migration to encrypted passwords

To assist with migration from unencrypted to encrypted client passwords, Samba offers a mechanism to automatically update client passwords as they connect.

If you have an existing population of Samba clients using unencrypted passwords, such as Windows 95 or Windows NT pre-service pack 3, and you wish to improve your network security by changing to encrypted passwords, you can configure Samba to automatically update the client's password upon logon.

This allows a site to migrate from plaintext password authentication to encrypted password authentication over an extended period and without forcing all users to reenter their passwords via smbpasswd at the time the change is made.

1. To start the migration process, edit your smb.conf file and add the following to the `[global]` section:

   ```
   [global]
   update encrypted = yes
   ```

2. In order for this parameter to work correctly the *encrypt passwords* parameter must be set to *no* when *update encrypted* is set to *yes*.

   ```
   encrypted passwords = no
   ```

Once all users have encrypted representations of their passwords in the smbpasswd file, reconfigure the smb.conf parameters as described in the following steps:

1. Reverse the *update encrypted* parameter to stop the migration process

   ```
   [global]
   update encrypted = no
   ```

If you need to maintain both encrypted and unencrypted client access on your system, you can use Samba support for multiple NetBIOS aliases or include client-specific configuration in smb.conf.

5.2.4 Password synchronization

Samba offers a parameter, unix password sync, which controls whether Samba attempts to synchronize the UNIX password with the SMB password when the encrypted SMB password in the smbpasswd file is changed. If this is set to true, the program specified in the *passwd program* parameter is run with root authority to allow the new UNIX password to be set without access to the old UNIX password (because the SMB password has been encrypted, we do not have access to the clear text of the old password, only the new one). By default, this parameter is set to *false*.

Along with this parameter, you have two others: passwd program and passwd chat, which let you define the command to run and its parameters to change the password.

5.3 Joining an existing domain

Since Version 1.9.18, Samba has included the ability to authenticate users against a remote password server, whether this is another Samba server or a Windows NT server. This was called *server-level* security and was configured by way of the *security=server* parameter in smb.conf. Server-level security has some limitations: It only returns a simple success/failure on password authentication and must maintain a connection with the password server for the duration of the client connection.

Samba Version 2.0.0 introduced *domain-level* security, which allows the Samba server to act as a member server in an existing domain. This is configured via the *security=domain* parameter in smb.conf. Domain-level security has several advantages over server-level security: Authentication returns the full set of user attributes (not just success/failure), and there is participation in domain trust relationships and reduced load on the password server (no unnecessary connection).

When a client attempts to access the server, Samba contacts the remote password server with the user's username and password. If the password is accepted by the remote password server, Samba grants the client access to the resources it requested.

Note

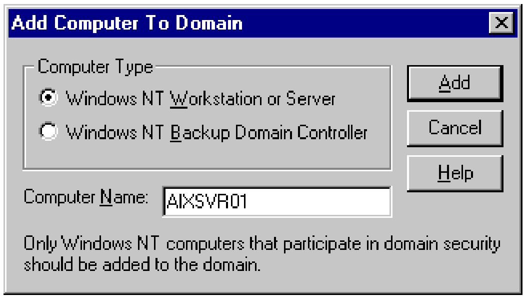
With domain-level and server-level security, you still need to create local AIX accounts before your users can access the Samba server. This allows AIX to associate files created with Samba with the local user's AIX account.

5.3.1 Adding a Samba server to an NT 4.0 domain

In order for a Samba server to join an NT 4.0 domain, you must first add the NetBIOS name of the Samba server to the Domain using the Server Manager for Domains tool (srvmgr.exe). This creates the machine account in the Primary Domain Controller's (PDC) System Administration Manager (SAM). You will need Domain Administrator privileges to accomplish this. Perform the following steps:

1. On a Windows client; Run the Server Manager for Domains tool, svrmgr.exe, and from the menu, select **Computer -> Add to Domain**.

2. Enter the NetBIOS name of the Samba server you wish to add. The *Computer Type* should be *Windows NT Workstation or Server*.



Add Computer To Domain

Computer Type

● Windows NT Workstation or Server

○ Windows NT Backup Domain Controller

Computer Name: AIXSVR01

Only Windows NT computers that participate in domain security should be added to the domain.

Figure 69. Add Computer To Domain - Server Manager for Domains

Your Samba server should now appear in the browse list for this domain.

5.3.2 Adding a Samba server to an Active Directory domain

Windows 2000 supports a *mixed-mode* domain model, which is, supposedly, 100 percent backwards-compatible with the pre-Windows 2000 domain model. This allows us to use a very similar process when joining the Active Directory domain as a member server.

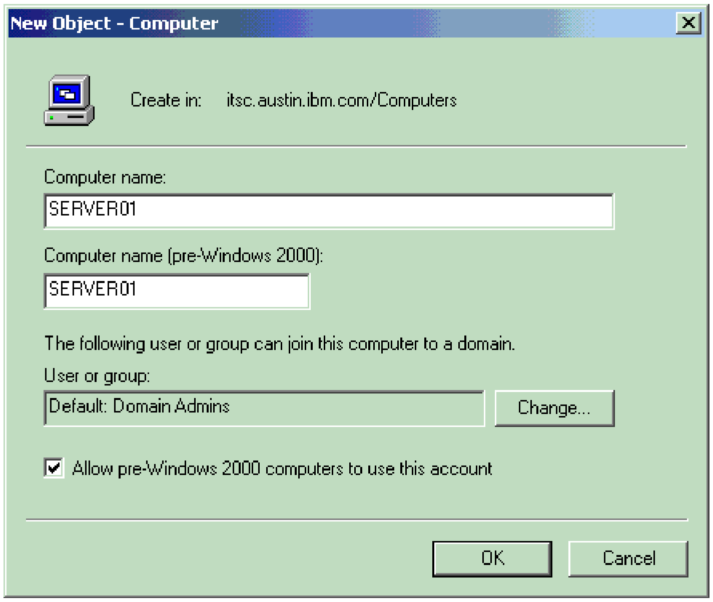
Just as with an NT 4.0 domain, you must add the NetBIOS name of the Samba server to the Active Directory before configuring Samba. This creates the machine account in the Active Directory database. You will need Domain Administrator privileges to accomplish this.

The following description can be found on the Web site, `http://web.mit.edu/pismere/directory-services/migration-4to5.html`:

Windows NT supports a mixed environment of Windows NT 5.0 Active Directory domain controllers and Windows NT 4.0 domain controllers. Customers can migrate at their own pace, based on business needs. Down-level clients will think they are accessing Windows NT 4.0 domain controllers. Windows NT Workstation and Windows® 95 clients that do not have the Active Directory access software will be able to log on to Active Directory domain controllers by using Windows NT LAN Manager (NTLM) challenge/response authentication.

1. On a Windows 2000 client, either manually run the *Server Manager for Domains* tool (svrmgr.exe), or, from the Start menu, select **Start -> Programs -> Administrative Tools -> Active Directory Users and Computers**.

2. From within the *Active Directory Users and Computers* tool, click the right-hand button in the *Computers* folder, and select **New -> Computer**.
3. Next, enter the NetBIOS name of the Samba server you wish to add. Select the **Allow pre-Windows 2000 computers to use this account** option as shown in Figure 70.



New Object - Computer

Create in: itsc.austin.ibm.com/Computers

Computer name: SERVER01

Computer name (pre-Windows 2000): SERVER01

The following user or group can join this computer to a domain.

User or group: Default: Domain Admins

☑ Allow pre-Windows 2000 computers to use this account

Figure 70. Adding Samba to an Active Directory domain - Users and Computers

Your Samba server should now appear in the browse list for this domain.

5.3.2.1 Create a machine account in the domain

Assume you have a Samba 2.0.x server with a NetBIOS name of SERVER01 and are joining an NT domain called DOMAIN01, which has a PDC with a NetBIOS name of DOMPDC and two backup domain controllers with the NetBIOS names, DOMBDC1 and DOMBDC2.

1. In order to join the domain, first, stop all Samba daemons and run the following command:

   ```
   smbpasswd -j DOMAIN01 -r DOMPDC
   ```

   We are joining the domain, DOMAIN01, with DOMPDC as the PDC for that domain (the only machine that has write access to the domain SAM database). If this is successful, you will see the following message in your terminal window (see the smbpasswd man page for more details):

   ```
   smbpasswd: Joined domain DOM.
   ```

This command goes through the machine account password change protocol then writes the new (random) machine account password for this Samba server into a file in the same directory in which a smbpasswd file would be stored (normally, /usr/local/samba/private).

The filename looks like this:

```
<NT DOMAIN NAME>.<Samba Server Name>.mac
```

The .mac suffix stands for machine account password file; so, in our example above, the file would be called:

```
DOMAIN01.SERVER01.mac
```

This file is created and owned by root and is not readable by any other user. It is the key to the domain-level security for your system and should be treated as carefully as a shadow password file.

5.3.2.2 Configure the Samba server

Before restarting the Samba daemons, you must edit your smb.conf file to tell Samba it should now use domain-level security. Perform the following steps:

1. Alter the security parameter in the [global] section of your smb.conf to read:

   ```
   security = domain
   ```

2. Next, change the workgroup parameter to read:

   ```
   workgroup = DOMAIN01
   ```

3. You must also have the encrypt passwords parameter set to *yes* in order for your users to authenticate to the NT PDC.

   ```
   encrypt passwords = Yes
   ```

4. Finally, add (or modify) the password server parameter to read:

   ```
   password server = DOMPDC DOMBDC1 DOMBDC2
   ```

   These are the primary and backup domain controllers that Samba will attempt to contact in order to authenticate users. Samba will try to contact each of these servers in order; so, you may want to rearrange this list in order to spread out the authentication load among domain controllers.

   Since Samba Version 2, you can also enter the asterisk character (*) to direct Samba to broadcast, or you can use a WINS database to find domain controllers to authenticate against. It is probably more secure to manually define the password servers. If you trust your clients implicitly (this is probably unwise), you may use the %m substitution to authenticate against the connecting client.

Security note

Using a password server means your Samba server (and AIX file system) is only as secure as your password server. Do not choose a password server that you don't completely trust.

5. Finally, restart your Samba daemons and try to connect to your Samba server using a valid Domain username and password.

Remember, even with domain-level security, you still need an AIX account on the Samba server, although you do not need the ability to log in to AIX. If you have any difficulty, examine Samba's log files while attempting to connect.

5.4 Using Samba as a primary domain controller (PDC)

A Primary Domain Controller is the central source for authentication in a SMB network Domain. Microsoft's Windows NT Server is the most common example of a PDC. The main difference between a Workgroup and a Domain is that in a Workgroup each client is responsible for its own security, while the PDC is responsible for security in a Domain.

Samba only provides limited PDC functionality, either restricted to some client types in the stable 2.0.x branch, or full PDC functionality in the experimental TNG branch. The forthcoming release of Samba 3.0 will provide full PDC functionality for all clients.

Note

AIX may not be suitable for use as a PDC in some environments due to its eight character limit on usernames. The *workstation trust account* username must consist of the hostname of the client PC appended with the $ character. This effectively restricts the membership of a Samba Domain using AIX as the PDC to clients with hostnames of no more than seven characters.

5.4.1 Configuring Samba 2.0.x

The 2.0.x branch of Samba only provides Domain Logon functionality for Windows 95 & 98 clients. It *does not* support Domain Logons for Windows NT or Windows 2000 clients because this requires full PDC functionality, which is not available in the 2.0.x branch. If you need to support Windows NT and 2000 clients in a production environment, you should either wait until the Samba 3.0 PDC code is released or consider using a Windows NT PDC.

To configure Samba 2.0.x to provide PDC-like (*Domain Logon)* functionality for Windows 95/98 clients *only*, perform the following procedure:

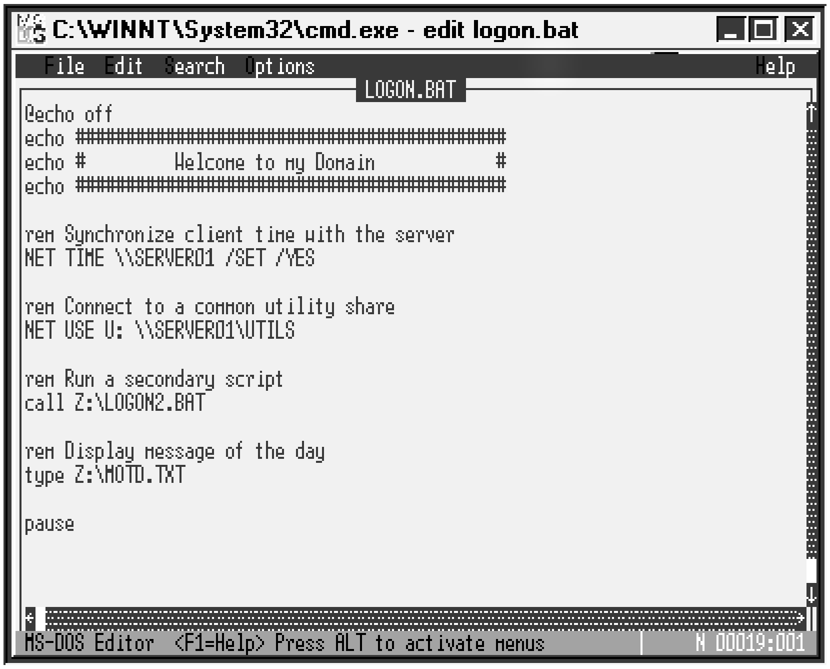
1. Edit smb.conf and configure Samba to provide Domain Logons. Use user-level security, and only accept encrypted passwords:

```
[global]
   domain logons = yes
   logon script = logon.bat
   security = user
   encrypt passwords = yes
```

The logon script can also include any of the standard substitution variables. For example:

```
   logon script = %U.bat
```

would provide every user with their own individual logon script (of course, you then need to create these logon scripts). Let us now create a simple logon script (you should use a PC editor so the file contains the correct CR/LF line terminations for execution on the client PC).


C:\WINNT\System32\cmd.exe - edit logon.bat
File
Edit
Search
Options
Help
LOGON.BAT

```
@echo off
echo ###########################################
echo #        Welcome to my Domain             #
echo ###########################################

rem Synchronize client time with the server
NET TIME \\SERVER01 /SET /YES

rem Connect to a common utility share
NET USE U: \\SERVER01\UTILS

rem Run a secondary script
call Z:\LOGON2.BAT

rem Display message of the day
type Z:\MOTD.TXT

pause
```

MS-DOS Editor <F1=Help> Press ALT to activate menus
N 00019:001

Figure 71. Sample domain logon script

You can, of course, make these scripts as complex as you want. They can be written in any scripting language that is executable by your clients. You must save the script to the netlogon share and ensure the client can read the logon script.

The client will map the netlogon share to the local Z: drive during the logon process. You can access the Z: to call other commands from within the script. The Z: drive will automatically disconnect after the script has completed.

2. Next, configure Samba to act as the Master Browser. Add the following entries to the `[global]` section in smb.conf:

```
[global]
   domain master = yes
   local master = yes
   preferred master = yes
   os level = 65
```

3. Next, identify a WINS server and configure your client to reference that server. This could either be a Windows NT WINS server or a Samba WINS server. Add the following entry to the `[globals]` section of smb.conf if you want to use Samba as the WINS server.

```
[global]
   wins support = yes
```

4. Edit smb.conf and create a share called *netlogon*. This share will contain client logon scripts and client policy files. It should be a read-only share.

```
[netlogon]
   path = /usr/local/samba/netlogon
   writable = no
   guest ok = no
```

5. Finally, ensure that your client has a username in smbpasswd and attempt a Domain Logon from your Windows 95/98 client.

Remember, you still need an AIX account on the Samba server and an entry in smbpasswd, although you do not need the ability to log in to AIX. If you have any difficulty, examine Samba's log files while attempting to connect.

5.4.2 Configuring Samba_TNG (2.1.0 alpha 0.8)

The TNG branch of Samba is the pre-alpha development version. Although it adds much-improved Domain Controller functionality to support Windows NT and Windows 2000 clients, it also lacks significant features available in the 2.0.x branch, such as the ability to serve Windows 95/98 clients. We have mentioned this here as an aid for those interested in experimenting with this rapidly-evolving product. The forthcoming Samba 3.0 will include the best features from both the 2.0.x and TNG branches.

Note

The TNG branch of Samba is still experimental, unstable code and should not be used in a production environment!

To configure Samba TNG to provide PDC (*Domain Logon)* functionality for Windows NT and Windows 2000 clients *only*, perform the following procedure:

1. Retrieve the latest Samba_TNG code via CVS as shown in Chapter 1, “Introduction to Samba” on page 1.
2. Compile and install the necessary Samba files. Take care not to overwrite an existing Samba installation.

   ```
   ./configure --prefix=/usr/local/samba-tng --disable-shared
   make
   make install
   ```

   In testing we experienced problems with shared library support for TNG under AIX. Use the `--disable-shared` parameter to compile TNG without support for shared libraries.

   We also had some difficulty compiling TNG with the IBM Visual Age C 5.0 compiler, even though it had compiled the 2.0.x code flawlessly. The TNG code compiled successfully with GCC 2.95.2
3. Because "make install" doesn't create all necessary files, you must create some files by hand.

   ```
   mkdir /usr/local/samba-tng/private
   mkdir /usr/local/samba-tng/profiles
   mkdir /usr/local/samba-tng/netlogon
   touch /usr/local/samba-tng/private/smbpasswd
   ```

   Change the mode for the profiles directory to 1777 so that Samba can create subdirectories for any user.

   ```
   chmod 1777 /usr/local/samba-tng/profiles
   ```
4. Next, create a suitable smb.conf file for use as a PDC.

```
[global]
        workgroup = SAMBA_TNG
        netbios name = SERVER01
        encrypt passwords = Yes
        time server = Yes
        logon script = login.bat
        logon path = `\\SERVER01\profile\%U'
        logon drive = M:
        logon home = `\\SERVER01\%U''
        domain logons = Yes
        os level = 65
        preferred master = Yes
        domain master = Yes
        wins support = Yes

[homes]
        comment = Users' home directories
        read only = No
        browseable = No

[netlogon]
        comment = PDC netlogon share
        path = /usr/local/samba/netlogon

[profile]
        comment = Profile share
        path = /usr/local/samba/profile
```

From AIX, create a user account for the Workstation Trust Account required for any workstation we wish to join our new Domain. The username for the Workstation Trust Account must be identical to the hostname of the connecting client (and less than seven-plus-one characters).

```
mkuser gecos='a workstation trust account' rlogin='false' client1\$
```

Next, create a password for the Workstation Trust Account. Initially, this password is simply the clients hostname. After the client first connects to the Domain, it will reset this password to a random value.

```
smbpasswd -a -m client1
```

This will create an entry in the smbpasswd file similar to the following:

```
client1$:uid:<LM passwd hash>:<NT passwd hash>:[W         ]:LCT-XXXXXXXX:
```

Security Note

The smbpasswd file contains two encrypted hashes of the user's password. Due to the nature of the SMB/CIFS challenge-response authentication protocol, the password hash can be used to impersonate a user on the network.

The smbpassword file *must* only be readable by the root user! By default it is in the private directory, which has read and traverse access restricted to the root user, with the smbpasswd file in read/write mode for root.

5.4.3 Obtaining NT domain administration tools

Assuming that your Domain is hosted entirely on Samba servers and you have not purchased a single Windows NT Server license, you may not have access to the client side administration tools. Fortunately, these tools are available free for download from Microsoft's Internet site.

- Server Manager, User Manager for Domains, and Event Viewer are available in a package, called Nexus, which is intended for installation on Windows 95 systems. They can be downloaded from the following URL:

  `ftp://ftp.microsoft.com/Softlib/MSLFILES/NEXUS.EXE`

- The Windows NT 4.0 tools, User Manager for Domains, and Server Manager are also available for download at the following URL:

  `ftp://ftp.microsoft.com/Softlib/MSLFILES/SRVTOOLS.EXE`

- The Windows NT Policy Editor is available as part of the Zero Administration Kit, and is available for download from the following URL:

  `http://www.microsoft.com/windows/zak/getzak.htm`

5.5 Windows 95/98 network logons

Samba supports Windows 95/98 network logons and roaming profiles. This means that a Windows 95/98 machine can log into the network by authenticating a users's password against the password database in Samba rather than Windows NT server. It also means that Windows95/98 can automatically retrieve a user's roaming profile from the Samba server.

When a Windows95/98 machine wishes to connect to the network, it broadcasts a request and consults WINS for the logon server for a particular NT domain. The first server that replies to the request processes the logon validating the password using whatever password authentication Samba has been configured to use.

5.5.1 Configuring Samba for Windows 95/98 network logons

The following steps are used to configure Network logons in Samba:

1. Configure security = user or security = server for domain logons to work correctly. Share level security will not work correctly.
2. Set up Samba to be a master browser.
3. Set up a WINS server for the environment. If a Windows NT WINS server is available, use that; otherwise, configure Samba to be a WINS server.
4. Configure all clients to use the WINS server.
5. Create a share, called [netlogon]. This share should be readable by all users and, probably, should not be writable. This share will contain the network logon script(s) and the CONFIG.POL file, which is used to configure system policies.
6. Create a logon script using a Windows editor, and place it in the [netlogon] directory. For example:

   net use U: \\lv3030d\netbench

   net use V: \\lv3030d\homes

   net use lpt2: \\lv3030d\optra
7. Use the Policy editor tool in Windows95/98 to create a CONFIG.POL policy file place it in the [netlogon] directory.
8. After changes in smb.conf have been made (either through SWAT or by manually editing the file), issue the `kill -9` command on the `nmbd` and `smbd` process-numbers.

Let us look at some Samba parameters that apply to these Net Logons:

domain logons If set to true, the Samba server will serve Windows 95/98 Domain logons for the workgroup it is in. For more details on setting up this feature, see the file, DOMAINS.txt, in the Samba documentation directory docs/ shipped with the source code.

Note that Win95/98 Domain logons are NOT the same as Windows NT Domain logons. NT Domain logons require a Primary Domain Controller (PDC) for the Domain. In a future release, it is intended for Samba to be able to provide this functionality for Windows NT clients as well.

Default:
domain logons = no

Example:
domain logons = yes

logon script This parameter specifies the batch file (.bat) or NT command file (.cmd) to be downloaded and run on a machine when a user successfully logs in. The file must contain the DOS style cr/lf line endings. It is recommended that you use a DOS-style editor to create the file.

The script must be a relative path to the [netlogon] service. If the [netlogon] service specifies a path of /usr/local/samba/netlogon, and logon script = STARTUP.BAT, the file that will be downloaded is: /usr/local/samba/netlogon/STARTUP.BAT.

The contents of the batch file is entirely your choice. A suggested command would be to add NET TIME \\SERVER /SET /YES to force every machine to synchronize clocks with the same time server. Another use would be to add NET USE U: \\SERVER\UTILS (for commonly-used utilities) or, for example, NET USE Q: \\SERVER\ISO9001_QA.

Note that it is particularly important not to allow write access to the [netlogon] share or to grant users write permission on the batch files in a secure environment because this would allow the batch files to be arbitrarily modified and security to be breached.

This option takes the standard substitutions allowing you to have separate logon scripts for each user or machine.

Note that this option is only useful if Samba is set up as a logon server.

Default:
None

Example:
logon script = scripts\%U.bat

The following example configuration appears in the smb.conf file:

```
[global]
.
.
.
security = user
local master = yes
domain logons = yes
wins server = 192.9.200.1
domain logons = yes
logon script = logon.bat
.
.
.
[netlogon]
path = /usr/local/samba/netlogon
read only = yes
guest ok = no
```

5.5.2 Enabling network logon in Windows 95/98

To configure Network logons in Windows 95/98, select **Control Panel -> Network -> Client for Microsoft Networks -> Preferences**. Select **Log on to NT Domain**, and then ensure that the Primary Logon is Client for Microsoft Networks. Press **OK**, and allow the computer to reboot.

Now, when Windows 95/98 boots up, it will show the Microsoft Network Login box containing [User , Password, Domain] instead of just [User, Password]. Enter the samba server's domain name (or any other domain known to exist, but bear in mind that the user will be authenticated against this domain and profiles downloaded from it, if that domain logon server supports it), user name and user's password.

5.5.3 Configuring Samba for roaming profiles

A roaming profile allows each user to store the contents of their Desktop and Start Menu on the Samba server; so, no matter which specific Windows 95/98 machine is used, a user will see the same desktop settings and Start Menu configuration.

If you are using a Samba server for the profiles, you must make the share specified in the logon path browseable. Windows 95 appears to check that it can see the share and any subdirectories within that share specified by the logon path option rather than just connecting straight away. It also attempts to create the components of the full path for you. If the creation of any component fails or if it cannot see any component of the path, the profile creation fails.

Let us look at some Samba parameters that apply to roaming profiles:

logon path This parameter specifies the home directory where roaming profiles (USER.DAT / USER.MAN files for Windows 95/98) are stored.

This option takes the standard substitutions allowing you to have separate logon scripts for each user or machine. It also specifies the directory from which the desktop, start menu, network neighborhood, and programs folders and their contents are loaded and displayed on your Windows 95/98 client.

The share and the path must be readable by the user for the preferences and directories to be loaded onto the Windows 95/98 client. The share must be writable when logged in for the first time in order for the Windows 95/98 client to be able to create the user.dat and other directories.

Thereafter, the directories and any of the contents can, if required, be made read-only. It is not advisable that the USER.DAT file be made read-only; rename it to USER.MAN to achieve the desired effect (a MANdatory profile).

Windows clients can sometimes maintain a connection to the [homes] share even though there is no user logged in. Therefore, it is vital that the logon path does not include a reference to the homes share (that is, setting this parameter to \\%N\HOMES\profile_path will cause problems).

This option takes the standard substitutions allowing you to have separate logon scripts for each user or machine.

Note that this option is only useful if Samba is set up as a logon server.

Default:

```
logon path = \\%N\%U\profile
```

Example:

```
logon path = \\%L\profiles\%U
```

5.5.4 Enabling roaming profiles in Windows 95/98

To configure a roaming profile in Windows 95/98, go to **Control Panel -> Passwords** and select the **User Profiles** tab. Select the required level of roaming preferences. Press **OK** and allow the computer to reboot.

For more information, see the DOMAIN.txt file in the Samba docs/textdocs directory.

5.5.5 Windows NT network logons

Microsoft does not publish the protocol that is used to implement Windows NT Domain authentication. The Samba team have reverse engineered the protocol from packet dumps.

As of Samba Version 2.0.0, support for Windows NT Domain Logons is still experimental, and Samba users could potentially have problems including corrupted NT registry; so, ensure that adequate backups have been performed before this task.

1. Obtain and compile Samba: see `http://samba.org/cvs.html`
2. Set up Samba with encrypted passwords: see ENCRYPTION.txt (you no longer need the DES libraries; ENCRYPTION.txt is current).
3. For each workstation, add a line to smbpasswd with a username of MACHINE$ and a password of machine. This process will be automated in further releases (but, for now, use smbpasswd -m machine_name).
4. If using NT server to log in, run the User Manager for Domains, and add the capability to Log in Locally to the policies, which you would have to do even if you were logging in to another NT PDC instead of a Samba PDC.
5. Set up the following parameters in smb.conf:

```
;  substitute your workgroup here
   workgroup = SAMBA

;  DO NOT add the redundant "domain sid = " parameter as this has
;  been superseded by code that automatically generates a random
;  sid for you.
;  domain sid = redundant.

;  tells workstations to use SAMBA as its Primary Domain Controller.
   domain logons = yes
```

6. Make sure Samba is running before the next step is carried out. If this is your first time, you might like to switch the debug log level to about 10. The NT pipes produces output when decoding requests and generating

responses, which would be particularly useful to see in tcpdump at some point.

7. In the NT Network Settings, change the domain to SAMBA. Do not attempt to create an account using the other part of the dialog: It will fail at present.

   You should get a message saying "Welcome to the SAMBA Domain."

   Assuming you got the Welcome message, go through the obligatory reboot.

8. When pressing Ctrl-Alt-Delete, the NT login box should have three entries. If there is a delay of about twenty seconds between pressing Ctrl-Alt-Delete and the appearance of this login dialog, there might be a problem:

   The domain box should have two entries: The hostname and the SAMBA domain.

   Any local accounts are under the hostname domain from which you will be able to shut down the machine, and so on.

   Select the Samba domain and type in a valid username and password for which there is a valid entry in the Samba server's smbpasswd database. At present, to allow access to the domain, the password is ignored, but it is *not* ignored for accesses to Samba's SMB services; that is completely separate from the SAM Logon process. Even if you log in a user to a domain, your users will still need to connect to Samba SMB shares with valid username / passwords for that share.

5.6 Windows Internet Name Service (WINS)

Use of WINS (either Samba WINS or MS Windows NT Server WINS) is highly recommended. Every NetBIOS machine registers its name together with a name_type value for each of the several types of services it has available.

RFC 1001.txt describes, among other things, the implementation and use of a NetBIOS Name Service. NT server offers Windows Internet Name Service, which is fully RFC 1001/2 compliant but has had to take specific action with certain NetBIOS names in order to make it useful.

Windows Internet Name Server (WINS) is based on and compatible with the Netbios Name Server protocol (NBNS) and, therefore, is compatible with other implementations and RFCs. When a new NetBIOS service is made available on the network, such as a Windows machine booting or Samba getting started, the service must be registered with the WINS server if it is to be available to clients located on other subnets.

When a machine is a WINS client, it attempts to resolve a hostname by first checking with the WINS server. If a host is not registered with a WINS server, it will attempt to find the host using a broadcast, which may be responded to by a Master Browser. If the host is still not found, a *Computer or sharename could not be found* error is returned.

Samba can be used either as a WINS server that can be queried by Microsoft client, or it can be a WINS client and properly register itself with any WINS server.

Use of WINS will work correctly only if every client TCP/IP protocol stack has been configured to use the WINS server/s. Any client that has not been configured to use the WINS server will continue to use only broadcast-based name registration so that WINS may never get to know about it. In any case, machines that have not registered with a WINS server will fail the name-to-address lookup attempts by other clients and will, therefore, cause workstation access errors.

Let us look at parameters that apply to setting up a Samba WINS client:

wins server This specifies the IP address (or DNS name: IP address for preference) of the WINS server with which nmbd should register. If you have a WINS server on your network, you should set this to the WINS server's IP.

You should point this at your WINS server if you have a multi-subnetted network.

Note

You need to set up Samba to point to a WINS server if you have multiple subnets and wish cross-subnet browsing to work correctly.

See the documentation file, BROWSING.txt, in the docs/ directory of your Samba source distribution.

Default:

```
wins server =
```

Example:

```
wins server = 192.9.200.1
```

Let us look at parameters that apply to setting up a Samba WINS server:

wins support This boolean parameter controls whether the nmbd process in Samba will act as a WINS server. You should not set this to true unless you have a multi-subnetted network and you wish a particular nmbd to be your WINS server. Note that you should *never* set this to true on more than one machine in your network.

Default:

```
wins support= no
```

Example:

```
wins support = yes
```

dns proxy This specifies that nmbd, when acting as a WINS server and finding that a NetBIOS name has not been registered, should treat the NetBIOS name word-for-word as a DNS name and do a lookup with the DNS server for that name on behalf of the name-querying client.

Note that the maximum length for a NetBIOS name is 15 characters; so, the DNS name (or DNS alias) can, likewise, only be 15 characters at most.

nmbd spawns a second copy of itself to do the DNS name lookup requests, since doing a name lookup is a blocking action.

Also see the parameter wins support.

Default:

```
dns proxy = yes
```

Example:

```
dns proxy = no
```

Never use wins support = yes with wins server = a.b.c.d, particularly not using its own IP address.

Samba offers WINS server capabilities. Samba does not interact with NT server (WINS replication); so, if you have a mixed NT server and Samba server environment, it is recommended that you use the NT server's WINS capabilities instead of Samba's WINS server capabilities.

The use of a WINS server cuts down on broadcast network traffic for NetBIOS name resolution. It has the effect of pulling all the broadcast-isolated subnets together into a single NetBIOS scope across your LAN or WAN while avoiding the use of TCP/IP broadcast packets.

When you have a WINS server on your LAN, WINS clients will be able to contact the WINS server to resolve NetBIOS names. Note that only those WINS clients that have registered with the same WINS server will be visible. The WINS server can have static NetBIOS entries added to its database, but for the most part, NetBIOS names are registered dynamically.

WINS includes a method of replicating its database with other WINS servers. Samba cannot take part in such replication, but it is possible for Samba to replicate its WINS database with another Samba WINS server.

WINS also serves the purpose of forcing browse list synchronization by all Local Master Browsers (LMBs). LMBs must synchronize their browse list with the Domain Master Browser (DMB), and WINS helps the LMB identify its DMB. By definition, this will work only within a single workgroup. Note that the domain master browser has *nothing* to do with what is referred to as an MS Windows NT Domain. The latter is a reference to a security environment while the DMB refers to the master controller for browse list information only.

An alternative to WINS is to use broadcast over a local subnet, which would be responded to by a Local Master Browser, but this will not work across subnets. Another alternative is to use the LMHOSTS file on WINDOWS clients. The LMHOSTS file is similar to a UNIX /etc/hosts file and maps NetBIOS names to IP addresses.

For more information, see the BROWSING.txt and BROWSING-Config.txt file in the Samba docs/textdocs directory.

Chapter 6. AIX and Samba integration

AIX provides a number of advanced features to ease administration and increase the reliability and availability of services. It is possible to integrate Samba into existing AIX management systems and exploit the high availability of AIX and load-sharing extensions.

6.1 Using the System Resource Controller (SRC) with Samba

AIX provides the System Resource Controller (SRC) as an alternative to init to manage and control processes. The SRC allows us to manage a related group of processes as a subsystem. We can start, stop, or refresh a related group of processes with a single command, even on a remote host. This allows us to use a common interface to manage a multitude of unrelated processes.

The SRC creates a hierarchy of processes, comprising subsystem groups, subsystems, and subservers. A subsystem group is a functionally-related group of subsystems, while a subsystem is a process, or group of processes, designed to provide a particular function. A subserver is a low-level daemon spawned by a subsystem. A subsystem may have multiple subservers.

We gain the following abilities from using the SRC:

- Consistent user interface for start, stop, and status inquiries
- Logging of the abnormal termination of subsystems
- Notification program called at the abnormal termination of processes
- Tracing of a subsystem, a group of subsystems, or a subserver
- Support for control of operations on a remote system
- Refreshment of a subsystem, such as after a configuration data change

Further details on SRC configuration may be found in the online AIX documentation at the following URL:

```
http://www.rs6000.ibm.com/doc_link/en_US/a_doc_lib/aixbman/admnconc/sys
_res_overview.htm
```

6.1.1 Modifying Samba to work with the SRC

If we wish to define the Samba daemons as independent subsystems, we need to make a minor change to the Samba source code. It is also possible to define the Samba daemons as subservers of the existing inetd subsystem without changing the source code, as we will show for the SWAT daemon later.

Typically, the Samba daemons are started either from a script or under the control of inetd. When run from a script, the daemons, smbd and nmbd, are called with the -D parameter causing them to run in the background and listen for their own network connections. When they are run under the control of inetd, the Samba daemons remain running in the foreground and do not have to listen for their own network connections because inetd handles this for them.

The SRC expects the Samba daemons to run in the foreground and listen for their own network connections. Unlike inetd, the SRC cannot listen for network connections on behalf of client processes. If the Samba daemons detach into the background, the SRC will lose track of them.

Running Samba as an independent subsystem under the SRC also has the advantage of only having to parse the smb.conf file once at startup, not once for every new connection as is the case with inetd.

Unfortunately, SWAT does not have the ability to listen for its own network connections; therefore, it is unsuitable to run as an independent subsystem under control of the SRC. If you wish, you can still define SWAT as a subserver of the existing inetd subsystem.

Use the following procedure to modify the *smbd* daemon if you wish to define it as an independent subsystem with the SRC.

1. Save the following patch to a file in the Samba source tree. For example:

   `./samba-2.0.6/source/smbd/server.diff`

```
702c702
<               DEBUG(0,("standard input is not a socket, assuming -D option\n"));
---
>       /*      DEBUG(0,("standard input is not a socket, assuming -D option\n")); *
706c706,707
<       if (is_daemon) {
---
>       /* if (is_daemon) { */
>       else if (is_daemon) {
```

2. Apply the patch to the original Samba code. For example:

```
cd ./samba-2.0.6/source/smbd
patch -b server.diff server.c
```

   This will save the original file as *server.orig*.

Use the following procedure to modify the nmbd daemon if you wish to define it as an independent subsystem with the SRC.

1. Save the following patch to a file in the Samba source tree. For example:

   ```
   ./samba-2.0.6/source/smbd/server.diff
   ```

```
772c772
<     DEBUG(0,("standard input is not a socket, assuming -D option\n"));
---
> /*    DEBUG(0,("standard input is not a socket, assuming -D option\n")); */
776c776,777
<   if (is_daemon)
---
>   /* if (is_daemon) */
>   else if (is_daemon)
```

2. Apply the patch to the original Samba code. For example:

   ```
   cd ./samba-2.0.6/source/nmbd
   patch -b nmbd.diff nmbd.c
   ```

   This will save the original file as *server.orig*.

After recompiling the Samba source code and installing the new binaries, you can define the new Samba SRC subsystem group.

6.1.2 Defining the Samba subsystem group

Once we have compiled and installed the modified Samba binaries, we can define the new subsystem to the SRC. We can control the effective user ID that runs the Samba daemons, whether they restart on failure, and which signals the SRC will use to control them. For example:

```
mkssys -G samba -s smbd -p /usr/local/sbin/smbd -u 0 -R -S -n 15 -f 3
mkssys -G samba -s nmbd -p /usr/local/sbin/nmbd -u 0 -R -S -n 15 -f 3
```

If you wish, you can also define SWAT as a subserver of the existing inetd subsystem. This will allow you to control the SWAT subserver with the normal SRC commands. You will still need to configure the /etc/inetd.conf file as is normal for the SWAT process.

```
mkserver -s inetd -t swat -c 901
```

Remember to add an entry to the server’s rc scripts to automatically start the new Samba subsystem upon system boot. For example, add this entry to /etc/rc.local:

```
startsrc -g samba
```

6.1.3 Controlling the new Samba subsystem

The SRC can use either signals, sockets, or IPC message queues to communicate with its various subsystems. Since the Samba code only supports signals, which is a one-way method of communication, it is limited to only recognizing stop requests. The Samba subsystem cannot recognize long status, refresh, or trace requests.

- To start the new Samba subsystem group, enter:

  ```
  startsrc [-h remote_host] -g samba
  ```

  or, to start an individual subsystem, enter:

  ```
  startsrc [-h remote_host] -s smbd
  ```

  or, to start the SWAT subserver, enter:

  ```
  startsrc [-h remote_host] -t swat
  ```

  If you configured inetd to start the SWAT daemon, it will automatically start upon a client connection to the SWAT port.

- To check whether the new Samba subsystem group is running, enter:

  ```
  lssrc [-h remote_host] -g samba
  ```

  or, to check an individual subsystem, enter:

  ```
  lssrc [-h remote_host] -s smbd
  ```

  or, to check the SWAT subserver, enter:

  ```
  lssrc [-h remote_host] -t swat
  ```

  or, to view all subservers of the inetd subsystem, enter:

  ```
  lssrc [-h remote_host] -l -s inetd
  ```

- To stop the new Samba subsystem group, enter:

  ```
  stopsrc [-h remote_host] -g samba
  ```

  or, to stop an individual subsystem, enter:

  ```
  stopsrc [-h remote_host] -s smbd
  ```

  or, to stop the SWAT subserver, enter:

  ```
  stopsrc [-h remote_host] -t swat
  ```

If you wish to manage remote systems with SRC commands, the srcmstr daemon (see /etc/inittab) must be started with the -r flag and the /etc/hosts.equiv or .rhosts file must be configured to allow remote requests.

6.1.4 Notify on subsystem failure

The SRC can be configured to notify an Administrator in the event of a subsystem or subsystem group failure. If the SRC has been configured to respawn a failed subsystem, it will only notify if that subsystem fails to respawn.

The method of notification is left entirely to the Administrator because the SRC will execute any script nominated. The SRC passes the name of the failed subsystem as the first argument to the script and the name of the failed subsystem group as the second.

This could be used to e-mail the Administrator, raise a Tivoli alert, use smbclient to warn users that the server is experiencing difficulties, and so on.

Create the appropriate script, and then use the following command to monitor the Samba subsystem:

```
mknotify -n samba -m /usr/local/samba/bin/notify.sh
```

When a notify method is defined for both a subsystem name and a group name, the subsystem name takes precedence. You can remove an existing notification method with the `rmnotify <name>` command.

6.2 Managing Samba via SMIT

Often, you do not have a way to access the SWAT, but you want to administer your Samba server without using the command line. You can use the System Management Interface Tool (SMIT) to administer your Samba server, but you have to first add the menus that you want to use.

To build these menus, you first have to do a script with the menu customization; then, you should include this script in the Object Data Manager (ODM). System data managed by ODM includes:

- Device configuration information
- Display information for SMIT (menus, selectors, and dialogs)
- Vital product data for installation and update procedures
- Communications configuration information
- System resource information.

6.2.1 Preparing the environment

In order to not damage your SMIT menu, you can make a copy of the SMIT databases. The SMIT database path is /usr/lib/objrepos. Copy the files to another directory, for example, /tmp/smittest. The following is a list of the files that you need to copy:

- sm_cmd_hdr
- sm_cmd_hdr.vc
- sm_cmd_opt
- sm_cmd_opt.vc
- sm_menu_opt
- sm_menu_opt.vc
- sm_name_hdr
- sm_name_hdr.vc

You can use the following command to copy these files:

```
cp /usr/lib/objrepos/sm_* /tmp/smittest
```

Now, you have to change the value of the ODMDIR variable. The default value of this variable is ODMDIR=/etc/objrepos. You need to change this in order to work with SMIT in the new path:

```
export ODMDIR=/tmp/smittest
```

6.2.2 Adding a menu

Now that you have finished preparing the environment you can start the configuration of your new menu. In this section we will explain how you can add a menu called Samba under the Applications menu. Then, we will explain how you can build a menu to list your smb.conf file.

1. Go to /tmp/smittest directory:

   ```
   cd /tmp/smittest
   ```

2. Make a script (samba_menu.add) with the menu configuration. You can use the vi editor to do this:

   ```
   vi samba_menu.add
   ```

   The following is the content of the script:

```
          sm_menu_opt:
                  id_seq_num = "010"
                  id = "apps"
                  next_id = "samba"
                  text = "Samba"
                  text_msg_file = ""
                  text_msg_set = 0
                  text_msg_id = 0
                  next_type = "m"
                  alias = ""
                  help_msg_id = "0"
                  help_msg_loc = ""
                  help_msg_base = ""
    help_msg_book = ""
```

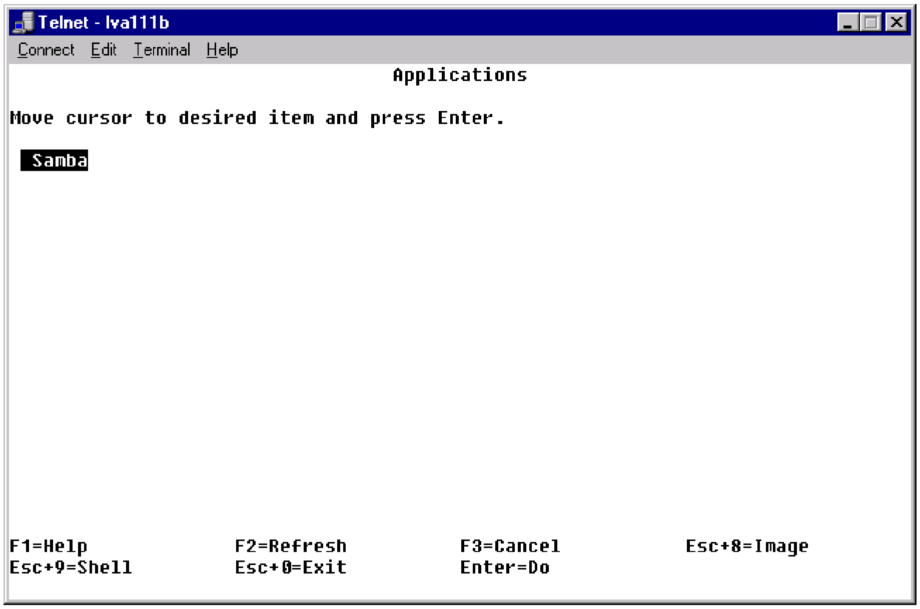
3. Add this menu to the ODM:

   ```
   odmadd samba_menu.add
   ```

4. Test the menu to make sure that it works. To start the SMIT in the current directory, you have to use the following command:

   ```
   smitty -o .
   ```

   Now, select **Applications** and press **Enter**. You should see a screen like the one shown in Figure 72 on page 134.



```
                                 Applications

Move cursor to desired item and press Enter.

  Samba

F1=Help              F2=Refresh           F3=Cancel            Esc+8=Image
Esc+9=Shell          Esc+0=Exit           Enter=Do
```

Figure 72. Applications

5. If you see the screen shown in Figure 72, your first menu was configured correctly; so, you can press **PF10** to exit from SMIT.

6. Now, we can start to build your second menu. You can use the vi editor to build this script:

   ```
   vi list_smbconf_menu.add
   ```

   The following screen shows the content of the script:

```
sm_menu_opt:
        id_seq_num = "010"
        id = "samba"
        next_id = "smbconf"
        text = "Samba server configuration file"
        text_msg_file = ""
        text_msg_set = 0
        text_msg_id = 0
        next_type = "d"
        alias = ""
        help_msg_id = "0"
        help_msg_loc = ""
        help_msg_base = ""
        help_msg_book = ""
```

7. Add the following menu to the ODM:

   ```
   odmadd list_smbconf_menu.add
   ```

8. Now, we can start to build your command menu. You can use the `vi` editor to build this script:

   ```
   vi list_smbconf.add
   ```

   The following is the content of the script.

```
sm_cmd_hdr:
        id = "smbconf"
        option_id = ""
        has_name_select = "n"
        name = "Samba server configuration file"
        name_msg_file = ""
        name_msg_set = 0
        name_msg_id = 0
        cmd_to_exec = "cat /usr/local/samba/lib/smb.con
        ask = "n"
        exec_mode = ""
        ghost = "y"
        cmd_to_discover = ""
        cmd_to_discover_postfix = ""
        name_size = 0
        value_size = 0
        help_msg_id = ""
        help_msg_loc = ""
        help_msg_base = ""
        help_msg_book = ""
```

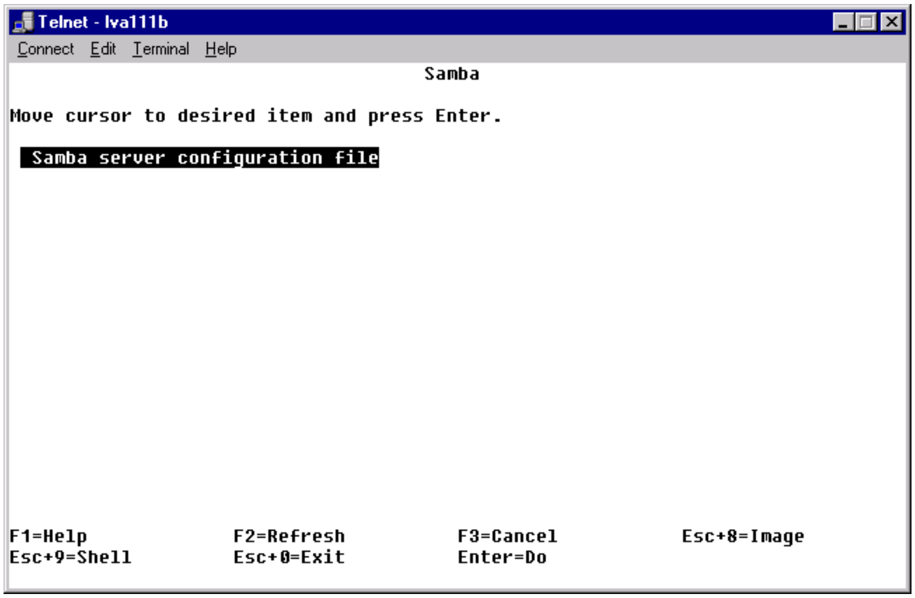
9. Add the following menu to the ODM:

   `odmadd list_smbconf.add`

10. You can test the menu to make sure that is working with the following:

    `smitty -o . samba`

    You should see the screen shown in Figure 73 on page 137.



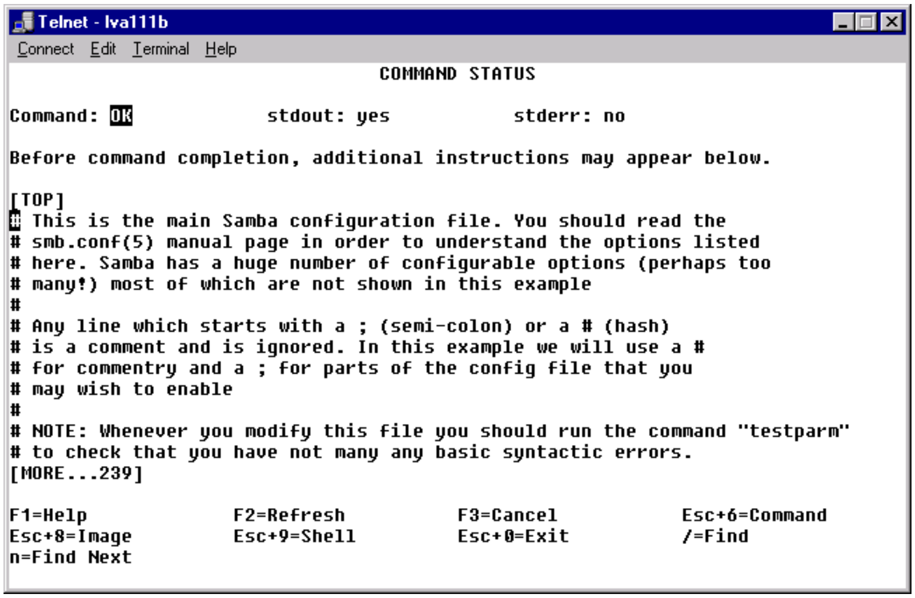
```
                                    Samba

Move cursor to desired item and press Enter.

  Samba server configuration file








F1=Help             F2=Refresh          F3=Cancel           Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

Figure 73. Samba

If you select the **Samba server configuration file** option, you should see a screen with the contents of the smb.conf file.

Note

If you want to build more menus, you have to change the options ID and next_id. These options contain the location of the menu. You also have to change the next_type option. You have to use m if the next type is a menu and d if it is a command. In the command menu, you need to change the cmd_to_exec option. This option contains the command that will be executed.



```
                            COMMAND STATUS

Command: OK            stdout: yes           stderr: no

Before command completion, additional instructions may appear below.

[TOP]
# 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.
[MORE...239]

F1=Help             F2=Refresh          F3=Cancel           Esc+6=Command
Esc+8=Image         Esc+9=Shell         Esc+0=Exit          /=Find
n=Find Next
```

Figure 74. Contents of the smb.conf file

6.2.3 Applying the new configuration.

If your customized SMIT is working fine, you have to apply this configuration on the original SMIT. The following is a procedure to apply the configuration:

1. Copy the SMIT files from /tmp/smittest to /usr/lib/objrepos:

   ```
   cp /tmp/smittest/sm_* /usr/lib/objrepos
   ```

2. Restore the initial value of the ODMDIR variable:

   ```
   export ODMDIR=/etc/objrepos
   ```

If you have successfully applied this configuration, you will see the Samba menus that you have created on the original SMIT.

6.2.4 Samba scripts

You can build some scripts and include them in SMIT to help you administer your Samba server. In the following screen, you can see a script that can help you perform some administration tasks in the Samba server. You can add the menus to execute these scripts using SMIT.

```
#!/usr/bin/ksh
#
# Start / Stop the Samba server and List the process
#

case "$1" in
  'start')
            ps -ef | grep -v grep | grep mbd > /dev/null
     STATUS=$?

     if [ $STATUS = 0 ]; then
        print "Samba server is running "
     else
        /usr/local/samba/bin/nmbd -D
        /usr/local/samba/bin/smbd -D
     ./smbctl status
     fi
    ;;
  'stop')
    ps -ef | grep nmbd | awk '{print $2}' | xargs kill > /dev/null 2>&1
    ps -ef | grep smbd | awk '{print $2}' | xargs kill > /dev/null 2>&1
    ./smbctl status
    ;;
  'status')
    ps -ef | grep -v grep | grep mbd
    STATUS=$?

    if [ $STATUS = 1 ]; then
      print "Samba server is stoped"
    else
      print "Samba server is running"
         fi
    ;;

    'restart')
        ps -ef | grep -v grep | grep mbd > /dev/null
        STATUS=$?

        if [ $STATUS = 1 ]; then
             print "Samba server is not running "
      else
             ./smbctl stop
             ./smbctl start
        fi
        ;;

     *)
    echo "Usage: $0 { start | stop | status | restart }"
    exit 1
    ;;
esac

exit
```

You can use some options on the script:

`start`:	Start the Samba server
`stop`:	Stop the Samba server
`status`:	Show the status
`restart`:	Restart the Samba server

6.3 Samba in a HACMP cluster

IBM High Availability Cluster Multi-Processing for AIX Enhanced Scalability (HACMP/ES) can be used to provide a highly-available infrastructure to support Samba for use in mission-critical environments.

AIX and HACMP offer many advanced functions to ensure the availability of a network service, such as Samba, including:

- Mature, industry-tested, clustering technology
- Supports clusters of up to 32 nodes in size
- IP address takeover between nodes
- MAC address takeover between nodes
- Can reconfigure an active cluster
- Multiple pre/post events for each cluster event

Due to the dynamic nature of NetBIOS name resolution, you can also use a WINS server to resolve the NetBIOS name of a failed-over Samba server without having to use IP/MAC address take-over.

Although HACMP can provide a highly available Samba server, you should also ensure that other parts of your network infrastructure are also highly available. For example, are your WINS servers replicated, are your password servers replicated, and do your nodes have multiple network paths to the cluster?

6.3.1 Installing an HACMP cluster

Installing an HACMP cluster, with proper planning and testing, is a complex and specialized endeavour. This section is only intended as a guide to configuring Samba for use in an existing HACMP cluster.

In our example, a two node Samba cluster might look something like Figure 75 on page 141.

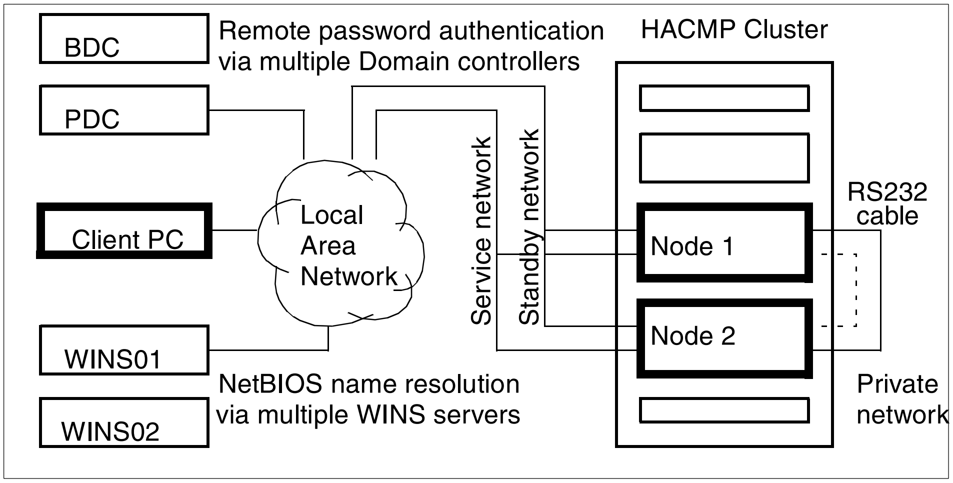


Figure 75. Simple Samba HACMP cluster example

As you can see, planning an HACMP cluster can rapidly become a complex affair. For more information on HACMP cluster technology, refer to the following URLs:

- High Availability Cluster Multi-Processing for AIX Documentation:

  `http://www.rs6000.ibm.com/doc_link/en_US/a_doc_lib/aixgen/hacmp_index.html`

- HACMP Enhanced Scalability Handbook:

  `http://www.redbooks.ibm.com/pubs/pdfs/redbooks/sg245328.pdf`

6.3.2 Configuring Samba in an HACMP cluster

Configuring and installing Samba in an existing HACMP cluster is relatively straightforward, although some understanding of HACMP concepts is essential.

6.3.2.1 Save the existing HACMP configuration

Before performing any work on the HACMP cluster, we should back up the existing configuration by taking a *snapshot*. This will allow us to restore the original configuration in case something goes wrong. Perform the following steps:

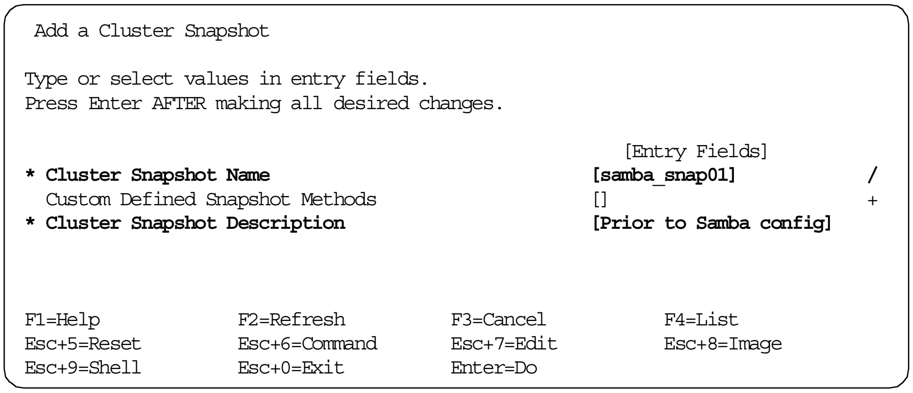
1. Start SMIT to configure HACMP with:

   ```
   smitty hacmp
   ```

   or, use the following fastpath for go directly to the correct menu:

```
smitty cm_add_snap.dialog
```

2. Enter a logical name for the snapshot file. For example, `samba_snap01`.



```
 Add a Cluster Snapshot

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                        [Entry Fields]
* Cluster Snapshot Name                              [samba_snap01]          /
  Custom Defined Snapshot Methods                    []                      +
* Cluster Snapshot Description                       [Prior to Samba config]



F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

3. Press **Enter** to save the snapshot.

   The snapshot will save to /usr/es/sbin/cluster/snapshots/.

6.3.2.2 Install and configure Samba

For Samba to successfully fail-over between multiple nodes in a cluster, each of those nodes must have the ability to access the disks, printers, and applications required. In an AIX environment, this can be achieved by connecting multiple nodes to an external SSA disk loop. This allows any node to vary on a required volume group and mount the file systems within.

A feature of HACMP, much like Samba, is the flexible way it can be implemented. You need to decide exactly what you wish to achieve before continuing. How many nodes will you have in your cluster? Will you run multiple Samba servers on multiple nodes or one Samba server on multiple nodes? What resources are already configured in HACMP?

In this example, we assume that you wish to run one Samba server on a cluster of two nodes using a remote PDC/BDC pair for authentication and remote WINS servers for name resolution.

1. On an external volume group, which is accessible to all nodes in the cluster, create a logical volume for the Samba executables and configuration with:

   ```
   mklv -y'samba-lv' -t'jfs' -c'2' external-vg01 4
   ```

   Create a file system on this logical volume. Set this file system to NOT automatically vary on and mount with the following:

   ```
   crfs -v jfs -d'samba-lv' -m'/usr/local/samba'
   ```

By installing Samba on an external volume group, we allow the Samba server's configuration to failover between nodes during a disaster.

2. On an external volume group, which is accessible to all nodes in the cluster, create one or more logical volumes to contain the data to be shared via Samba. Create file systems on these logical volumes. Set these file systems to NOT automatically vary on and mount. For example, enter:

   ```
   mklv -y'share-lv01' -t'jfs' -c'2' external-vg02 80
   ```

   Create a file system on this logical volume:

   ```
   crfs -v jfs -d'share-lv01' -m'/usr/samba_share_01'
   ```

   Set these file systems to NOT automatically vary on and mount.

3. Mount the newly created file systems on any one node with the following:

   ```
   mount /usr/local/samba
   mount /usr/samba_share_01
   etc.
   ```

The Concurrent Logical Volume Manager (CLVM) only supports raw logical volumes; so, we cannot concurrently mount JFS file systems between nodes.

Install and test Samba as you would a non-HACMP system. *Do not* configure Samba to start automatically, and do not configure inetd to start Samba. HACMP will be responsible for starting and stopping Samba.

1. Configure Samba with a smb.conf file similar to the example shown in the following screen:

   ```
   # Global parameters
   [global]
           workgroup = DOMAIN01
           netbios name = HASMB
           encrypt passwords = Yes
           security = domain
           password server = DOMPDC, DOMBDC
           wins server = WINS01, WINS02

   [test]
           comment = HA share on external volume group
           path = /usr/samba_share_01
           read only = No
           guest ok = Yes
   ```

   Refer to Chapter 2, "Installing Samba on AIX" on page 9, and Chapter 3, "Basic configuration" on page 15, for instructions on configuring Samba.

2. Ensure your clients can connect to the new Samba server.

3. Stop Samba, dismount the new file systems, and vary off any new volume groups before continuing with the HACMP configuration.

6.3.2.3 Create start/stop scripts for Samba

HACMP needs to be able to reliably start and stop the Samba daemons during cluster start/stop events. When a node running a Samba server is failed-over to another node in the cluster, we must ensure that the original Samba server halts so that we can free its resources and restart the Samba server with the same NetBIOS name on the replacement node.

Create a script to start the Samba daemons in a local directory on all nodes in the cluster. For example:

`/usr/sbin/cluster/scripts/ha_samba_start.sh`

```
#!/usr/bin/sh -f

print “Starting the Samba server...”

/usr/local/samba/bin/smbd -D
/usr/local/samba/bin/nmbd -D

# Or, if you are using the SRC subsystem
# startsrc -g samba
```

Create a script to stop the Samba daemons in a local directory on all nodes in the cluster. For example:

`/usr/sbin/cluster/scripts/ha_samba_stop.sh`

```
#!/usr/bin/sh -f

# Do our best to alert connected users

LIST=`/usr/local/samba/bin/smbstatus -b | tail +5 | awk '{print $3}'`

for CLIENT in $LIST
do
    cat /usr/sbin/cluster/scripts/samba_down.txt | \
        /usr/local/samba/bin/smbclient -M $CLIENT
done

print “Stopping the Samba server...”
kill -9 `cat /usr/local/samba/var/locks/smbd.pid`
kill -9 `cat /usr/local/samba/var/locks/nmbd.pid`

# Or, if you are using the SRC subsystem
# stopsrc -g samba
```

Although most HACMP configuration can be managed from a single node, the application start and stop scripts must be manually copied to each node in the cluster.

Samba 2.0.7 introduces a new configuration parameter, source environment, which can be used to dynamically set environment variables, and reconfigure your Samba server as it fails-over between nodes. The parameter accepts either the name of a text file to parse or a command to execute.

To read environment settings from a text file, simply enter the name of the text file to parse. The text file must be owned by root and not be world-writable. For example:

```
source environment = /usr/sbin/cluster/scripts/smb_env_vars
```

To execute a script and set environment variables from its output, enter the name of the script, prepended with a | symbol (a pipe or vertical bar). The script must not be world-writable and must reside in a directory that is not world-writable. For example:

```
source environment = | /usr/sbin/cluster/scripts/smb.conf.sh
```

The text file, or output from the script, should be formatted as per the output of the standard UNIX env(1) command. For example:

```
SAMBA_NETBIOS_NAME=myhostname
```

6.3.2.4 Create the Samba resource group

Next, we need to create a *resource group* for Samba in HACMP. Here, we define which nodes can host the Samba application and how it reacts to node failures and restorations.

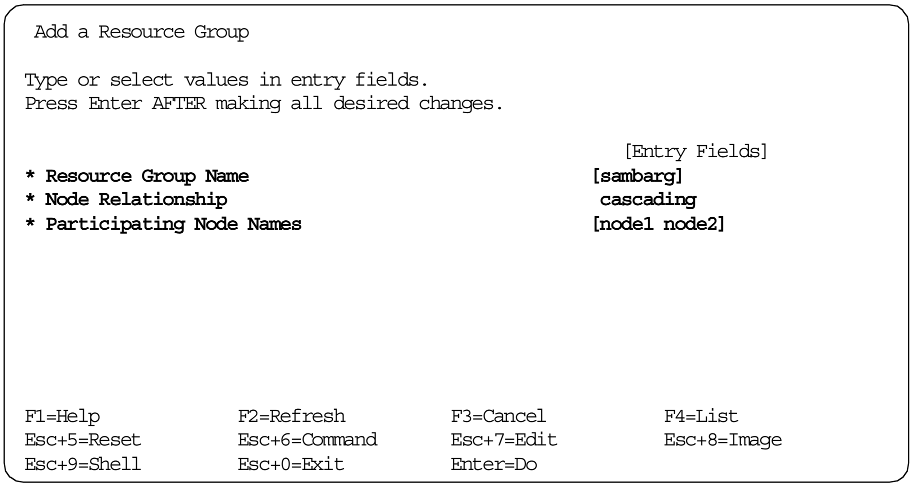
1. Start SMIT to configure HACMP with:

   ```
   smitty hacmp
   ```

   or, use the following fastpath for go directly to the correct menu:

   ```
   smitty cm_add_grp
   ```

2. Enter a logical name for the new Samba resource group. For example, enter `sambarg`.



```
 Add a Resource Group

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                      [Entry Fields]
* Resource Group Name                              [sambarg]
* Node Relationship                                 cascading
* Participating Node Names                         [node1 node2]







F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

The “Node Relationship” controls how this resource group will react to node failures and restorations. Nodes are assigned priority depending on their host name.

Cascading resources may be assigned to be taken over by multiple nodes in a prioritized manner. When a node fails, the active node with the highest priority acquires the resource. When the failed node rejoins, the node with the highest priority acquires the resource.

Rotating resources may be acquired by any node in its resource chain. When a node fails, the resource will be acquired by the highest priority standby node. When the failed node rejoins, the resource remains with its new owner.

For *Participating Node Names*, enter the names of every node in the cluster that you wish to be able to host the Samba application. For example:

```
node1 node2
```

3. Press **Enter** to save your changes.

6.3.2.5 Create the Samba application server

Next, we need to create an *application server* for Samba in HACMP. The Samba daemons must not automatically start upon system boot; instead, they will be started and stopped by HACMP. We need to define which scripts to run on cluster start and stop events to start and stop the Samba daemons. Perform the following steps:

1. Start SMIT to configure HACMP

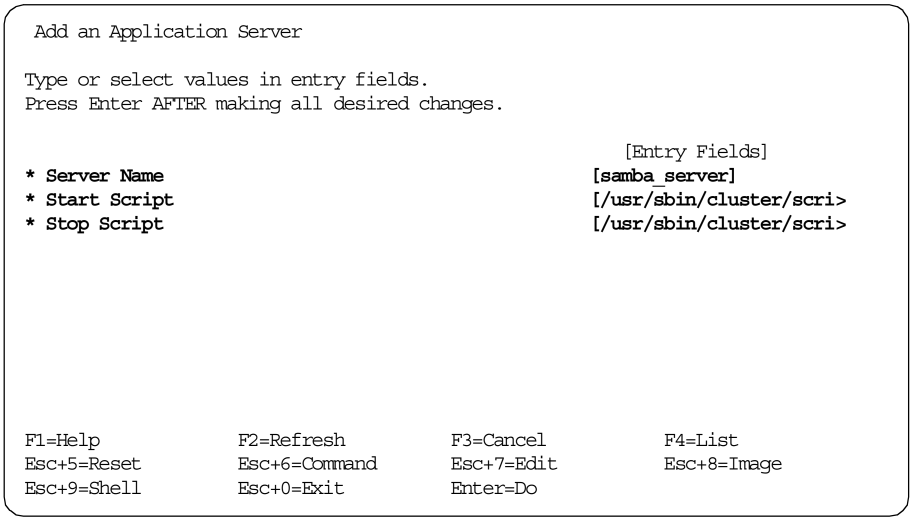
```
smitty hacmp
```

or, use the following fastpath for go directly to the correct menu

```
smitty claddserv.dialog
```

2. This is where we create the *application server* definition for Samba in HACMP.

   Enter a logical name for your Samba service. For example, enter: `samba_server`.



```
 Add an Application Server

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                          [Entry Fields]
* Server Name                                           [samba_server]
* Start Script                                          [/usr/sbin/cluster/scri>
* Stop Script                                           [/usr/sbin/cluster/scri>









F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

   Enter the full path to your Samba start and stop scripts. For example, enter:

```
/usr/sbin/cluster/scripts/ha_samba_start.sh
/usr/sbin/cluster/scripts/ha_samba_stop.sh
```

3. Press **Enter** to save your changes.

6.3.2.6 Configure the Samba resource group

Here, we associate file system and application resources with the new Samba resource group. Perform the following steps:

1. Start SMIT to configure HACMP:

```
smitty hacmp
```

   or, use the following fastpath for go directly to the correct menu:

```
smitty cm_cfg_res.select
```

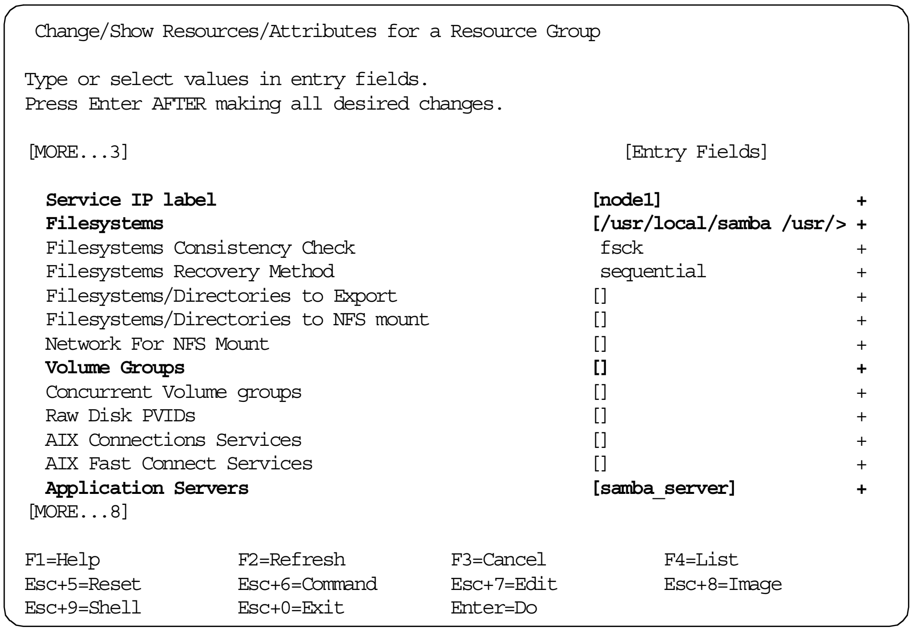
2. Select the new Samba resource group to configure.

3. We need to modify the following parameters to suit your local system:

- **Service IP label**

  The IP label (hostname) of the adapter, associated with the numeric IP address in the /etc/hosts file (if the address type is ip address).

  Enter the service IP address of the initial node to own this resource group.



```
 Change/Show Resources/Attributes for a Resource Group

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[MORE...3]                                            [Entry Fields]

  Service IP label                                   [node1]                +
  Filesystems                                        [/usr/local/samba /usr/> +
  Filesystems Consistency Check                       fsck                  +
  Filesystems Recovery Method                         sequential            +
  Filesystems/Directories to Export                  []                     +
  Filesystems/Directories to NFS mount               []                     +
  Network For NFS Mount                              []                     +
  Volume Groups                                      []                     +
  Concurrent Volume groups                           []                     +
  Raw Disk PVIDs                                     []                     +
  AIX Connections Services                           []                     +
  AIX Fast Connect Services                          []                     +
  Application Servers                                [samba_server]         +
[MORE...8]

F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

- **File systems**

  Enter the mount points of the file systems that are mounted when the resource is initially acquired.

  For example: `/usr/local/samba /usr/samba_share_01`

- **Volume Groups**

  Enter the names of the volume groups containing raw logical volumes or raw volume groups that are varied on when the resource is initially acquired. It is not necessary to enter the volume group names as they will be automatically varied on when their included file systems are mounted.

- **Application servers**

  Enter application servers that will be started by this resource group. These are the servers defined in the "Define Application Servers" section.

  For example: `samba_server`

4. Press **Enter** to save your changes.

6.3.2.7 Synchronize cluster resources

Finally, we need to synchronize the new HACMP configuration between all nodes in the cluster. This is essential to ensure that each node will have the latest configuration in case of a fail-over event. The other node(s) will be ignorant of our changes until this step is complete. We also need to synchronize any changes made at an AIX level between nodes, such as new file systems, volume groups, users, and application scripts.

Synchronize AIX configuration

We need to import any changes to the logical volume and file system definitions to every other node in the cluster. Although AIX *can* import these settings automatically during a failover, doing so now allows us to confirm their correct operation and reduces downtime during a disaster.

Use the following procedure to import changes made to Node1's logical volume layout to Node2. We can import the logical volume layout even while Node 1 has the volume group varied on and in use.

1. On Node 1, break the disk reservation locks on the already varied on volume group and leave it unlocked.

   ```
   vayonvg -b -u sambavg
   ```

2. On Node 2, import the logical volume definition.

   If the volume group is known to Node 2 and we only want to update the logical volume and file system definitions, use the following command:

   ```
   importvg -L sambavg hdiskXX
   ```

   If the volume group is *not* known to Node 2 and we want to import the entire volume group definition, use the following command:

   ```
   importvg -y sambavg -n hdiskXX
   ```

   Replace hdiskXX with the hdisk label of any disk in the volume group we wish to import. When a new volume group is imported, it will be set to automatically vary on. You must manually reset this to not vary on.

3. On Node 1, restore the disk reservation locks on the already-varied-on volume group:

   ```
   vayonvg sambavg
   ```

Application scripts need to be manually copied from the original node to each node in the cluster. Remember to set the correct ownership and file system permissions on the scripts. If you have changed user or group information, this will also need to be synchronized across the nodes.

Synchronize HACMP configuration

Use the following procedure to synchronize changes made to the HACMP configuration on Node 1, such as new resource groups, application servers, and so on, between all nodes in the cluster.

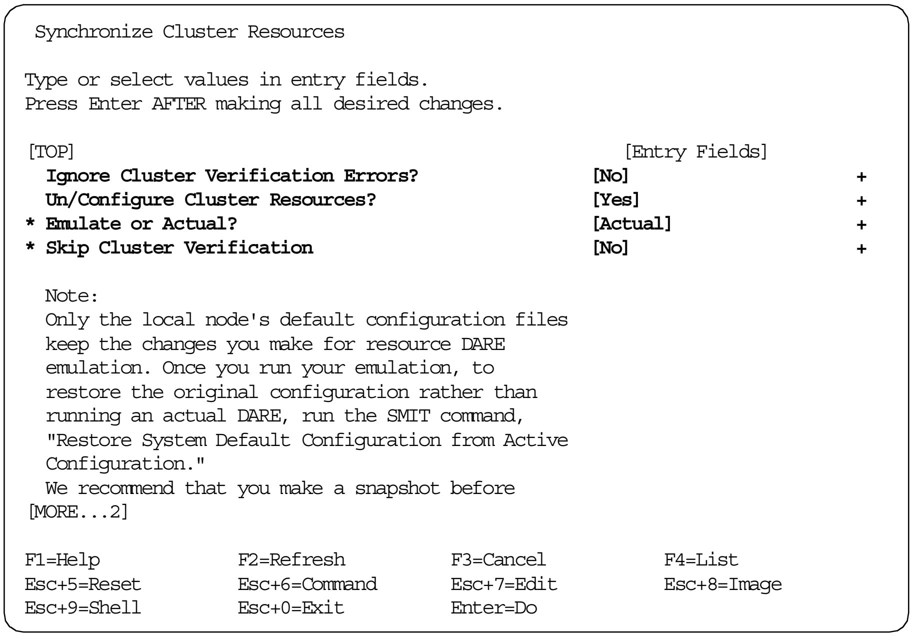
1. Start SMIT to configure HACMP:

   ```
   smitty hacmp
   ```

   or, use the following fastpath for go directly to the correct menu:

   ```
   smitty clsyncnode.dialog
   ```

2. From this menu, you can synchronize the cluster configuration.



```
 Synchronize Cluster Resources

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP]                                                  [Entry Fields]
  Ignore Cluster Verification Errors?               [No]                   +
  Un/Configure Cluster Resources?                   [Yes]                  +
* Emulate or Actual?                                [Actual]               +
* Skip Cluster Verification                         [No]                   +

  Note:
  Only the local node's default configuration files
  keep the changes you make for resource DARE
  emulation. Once you run your emulation, to
  restore the original configuration rather than
  running an actual DARE, run the SMIT command,
  "Restore System Default Configuration from Active
  Configuration."
  We recommend that you make a snapshot before
[MORE...2]

F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

3. Press **Enter** to synchronize the cluster.

The cluster verification utility will be run before the information is synchronized to all cluster nodes. The verification utility will verify that the cluster topology and/or cluster resources are properly configured. Under certain circumstances, it may be necessary to perform the synchronization even if the verification routines report an error. Be advised that the verification should be ignored only under conditions that are well understood by the cluster administrator.

6.3.2.8 Verify the HACMP configuration

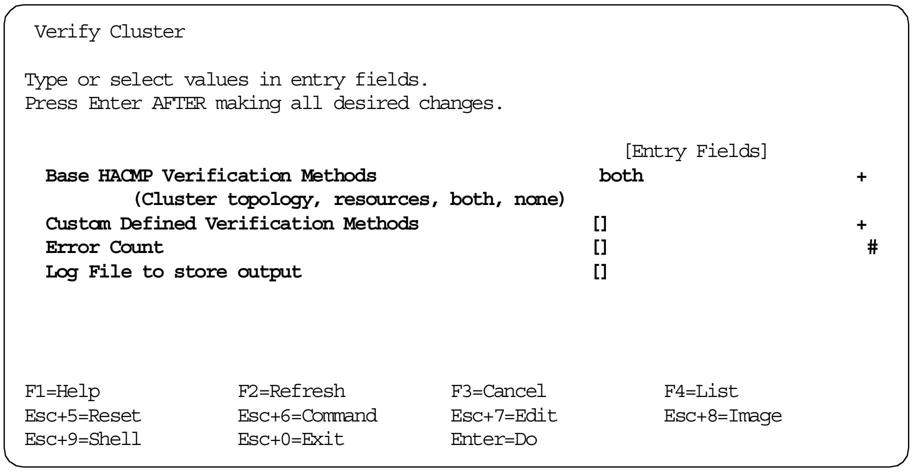
At this point, you should have correctly configured the Samba resource group and application server in HACMP, synchronized changes to AIX logical volumes and file systems, and copied the Samba start and stop scripts to each node in the cluster. We can verify the HACMP configuration from within SMIT. Perform the following steps:

1. Start SMIT to configure HACMP:

   ```
   smitty hacmp
   ```

   or, use the following fastpath to go directly to the correct menu:

   ```
   smitty clverify.dialog
   ```



```
 Verify Cluster

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                    [Entry Fields]
  Base HACMP Verification Methods                  both                +
          (Cluster topology, resources, both, none)
  Custom Defined Verification Methods              []                  +
  Error Count                                      []                   #
  Log File to store output                         []




F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

2. Press **Enter** to verify the cluster configuration.

After verifying the configuration, and correcting any errors, you should save another snapshot as shown in Section 6.3.2.1, “Save the existing HACMP configuration” on page 141.

6.3.2.9 Test Samba operation and HACMP failover

After you have correctly configured HACMP to support the Samba file server, you must now test Samba’s function in the stable and failed-over cluster.

After a node failure, HACMP will detect the loss of a cluster member, mount appropriate resources, and start the required services on another node. Although existing client connections are suspended during the (hopefully short) period between node failure and service restoration, clients should be able to transparently reconnect to the Samba server on its new node. Once the original node has been restored to service, the HACMP subsystem can be restarted. When the cluster realizes that the original node has returned, it can shut down Samba and free its resources on the current node, mount those resources, and start the Samba server on the original node.

You need to test both the fail-over of the Samba server between nodes and the ability of your client population to access the Samba server regardless of the node on which it is currently running.

Remember, if you are going to use a remote password server to authenticate client access, your Samba server will only be as available as the password server. You may wish to define multiple password servers and confirm their availability during node and network failure testing.

6.4 Using the SecureWay Network Dispatcher

The IBM SecureWay Network Dispatcher is a server load balancing software. It boosts the performance of servers by directing TCP/IP session requests to different servers within a group of servers. In this way, it balances the requests among all the servers. This load balancing is transparent to users and other applications. You can use SecureWay Network Dispatcher for applications that use the TCP/IP protocol. In this section we will explain how you can set up the Network Dispatcher server to balance the request among your samba server.

SecureWay Network Dispatcher consists of three components that can be used separately or together:

- **Dispatcher** - You can use the Dispatcher component by itself to balance the load on servers within a local area network or wide area network using a number of weights and measurements that are dynamically set by Dispatcher.
- **ISS** - You can use the Interactive Session Support (ISS) component by itself to balance the load on servers within a local or wide area network using a domain name server (DNS) round-robin approach or a more advanced user-specified approach. Load balancing is performed at the machine level. ISS can also be used to provide server load information to a Dispatcher machine. When used for load balancing, ISS works in conjunction with the DNS name server to map DNS names of ISS services to IP addresses. When used to provide server load information, a name server is not required.
- **CBR** - You can also use the Content Based Routing component to load balance based on the content of the client request.

In this section, we will cover the setup of the Dispatcher component, but you can find more information about the Dispatcher and the setup of the other components at the following URL:

```
http://www-4.ibm.com/software/network/dispatcher/library
```

6.4.1 Installing for AIX

Table 6 contains a list of the installp images to install for SecureWay Network Dispatcher.

Table 6. Installp images

Dispatcher (component, adminstration, license, and messages)	intnd.nd.driver intnd.nd.rte intnd.ndadmin.rte intnd.nd.license intnd.msg.nd.<language>.nd.rte intnd.msg.<language>.ndadmin.rte intnd.admin.rte intnd.msg.<language>.admin.rte
ISS (component, administration, license, and messages)	intnd.iss.rte intnd.issadmin.rte intnd.iss.license intnd.msg.<language>.iss.rte intnd.msg.<language>.issadmin.rte intnd.admin.rte intnd.msg.<language>.admin.rte
CBR (component, administration, license, and messages)	intnd.cbr.rte intnd.cbradmin.rte intnd.cbr.license intnd.msg.<language>.cbr.rte intnd.msg.<language>.cbradmin.rte intnd.admin.rte intnd.msg.<language>.admin.rte
User's Guide	intnd.doc.<language>

Perform the following steps to install SecureWay Network Dispatcher for AIX:

1. Log in as root.
2. Insert the product media, or, if you are installing from the Web, copy the install images to a directory.

3. Install the installation image. It is recommended that you use SMIT to install SecureWay Network Dispatcher for AIX because SMIT will ensure that all messages are installed automatically.

   Using SMIT, perform the folllowing steps:

   a. Select **Software Installation and Maintenance**.

   b. Select **Install and Update Software**.

   c. Select **Install Software Products at Latest Level**.

   d. Select **Install and update from all Available Software**.

   e. Enter The device or directory containing the installp images.

   f. On the *SOFTWARE to Install line, enter the appropriate information to specify options (or select **PF4**).

   g. Press **OK**.

When the command completes, press **Done**, and then select **Exit Smit** from the Exit menu or press **F12**. If using SMITTY, press **F10** to exit the program.

6.4.1.1 Configuring the Dispatcher component

We are going to use an example to explain how you can set up your Dispatcher component. We are going to use two SP nodes working as a Samba server and the SP Control Workstation working as a Dispatcher server as shown in Figure 76.

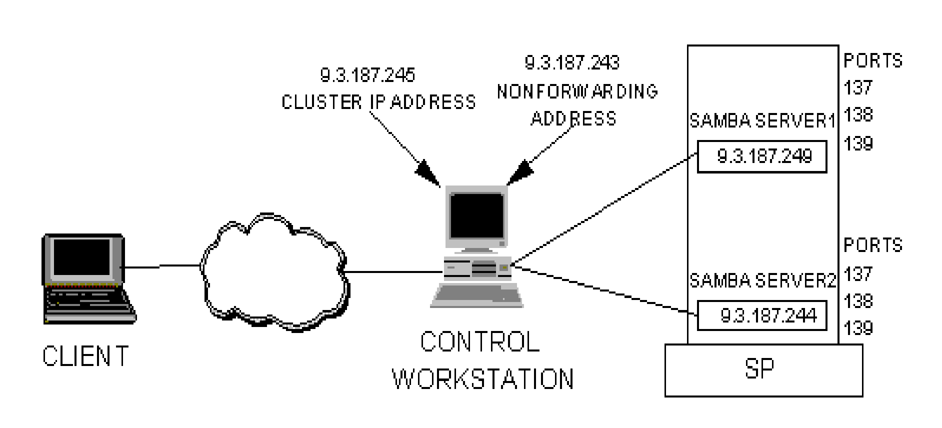


Figure 76. Dispatcher configuration

Perform the following steps to configure the Dispatcher component:

1. Run the following command as root:

```
ndserver
```

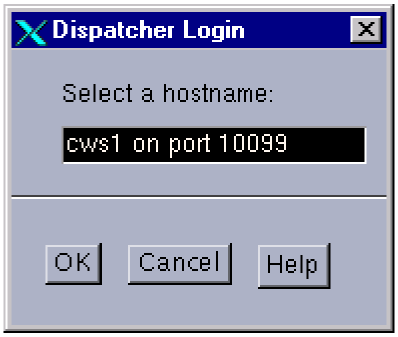
2. Start the graphical user interface (GUI):

   ```
   ndadmin
   ```

   The left side of the window displays a tree structure with SecureWay Network Dispatcher at the top level, and Dispatcher, ISS, and CBR as components. All of the components can be configured from the GUI. We will configure only the dispatcher component.

3. Click with the right mouse button on **Dispatcher** and click on **Connect to Host...**

   You will see a dialog box as shown in Figure 77.


Dispatcher Login

Select a hostname:

cws1 on port 10099

Figure 77. Dispatcher Login

4. Click on **OK**.

   Now that you are connected to the Dispatcher server, you should start the executor in order to configure the cluster.

5. With the right button mouse, click on **Host: <hostname>**, and then click on **Start Executor**.

   If you have a previous configuration file you can again right-click on **Host: <hostname>**, and then click on **Load New Configuration...**.

6. Click with the right mouse button on **Executor: <executor_ip_address>**, and then click on **Add cluster...**.

   You should see a dialog box prompting you to enter the IP Address of the cluster. This IP Address should be the one that your clients are going to use to reach the Samba server.

   Click on **OK** when you finish entering the IP Address.

   Now that you have a cluster defined, you should add the ports that you are going to use. You should add the ports numbered 137, 138, and 139.

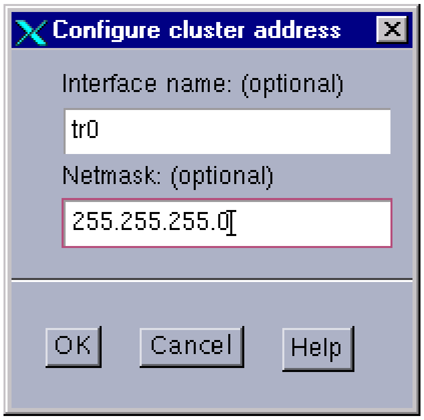
To add a port, you should click with the right button on **Cluster:<cluster_ip_address>**, and then click on **Add Port...**. Then, you should see a dialog box prompting you to enter the port number that you want to add.

You should repeat this to create the others ports necessary to the Samba server.

7. You should add the servers to the port that you have defined. You can add as many servers as you have running Samba. In our example, we use two servers, Samba server 1 and Samba server 2.

   To include a server in the port, you need to click with the right button on the port that you want to add to the server. Click on **Add Server...** and enter the IP address of the server that you want to add in the dialog box.

   When you finish configuring all the servers in all the ports that you have defined, you need to configure the Dispatcher server to accept traffic for the cluster address. Right mouse click on **Cluster:<cluster_ip_address>**, and then click on **Configure Cluster Address...**. You will see a dialog box as shown in Figure 78.



Interface name: (optional)

tr0

Netmask: (optional)

255.255.255.0

Figure 78. Configure cluster address

You can enter the interface name that you want to configure the cluster and netmask that you are going to use. Click on **OK** when you finish configuration.

You may now be able to ping the IP address of the cluster that you have defined. Try to do this to test your cluster configuration.

6.4.1.2 Configuring the Samba server

For the Samba server to work, you must set (or, preferably, alias) the loopback device (often called lo0) to the cluster address. The Dispatcher component does not change the destination IP address in the TCP/IP packet before forwarding the packet to a TCP server machine. By setting or aliasing the loopback device to the cluster address, the Samba server will accept a packet that was addressed to the cluster address.

> **Note**
>
> If your Dispatcher server and your Samba server are in the same machine, you should *not* set the alias loopback.

You can use the following command to set the alias loopback:

```
if config lo0 alias <cluster_ip_address> netmask <cluster_netmask>
```

You should set up the alias loopback in all the Samba server that you added to the cluster.

Now that your Netdispatcher server is working to load balace the request, you need to set up your Samba client machines to access the hostname and IP address that you have defined for the cluster address instead of directly accessing the Samba server.

6.4.1.3 Configuring NFS

If you are going to implement a solution using the Network Dispatcher, it is advisable to have all the Samba servers share the same disk. You can use the NFS to export a file system for your nodes and, in this way, share the files for your Samba servers.

You can configure the Network File System (NFS) to share your files between your Samba servers. The Network File System is a distributed file system that allows users to access files and directories located on remote computers and treat those files and directories as if they were local. For example, users can use operating system commands to create, remove, read, write, and set file attributes for remote files and directories.

NFS provides its services through a client-server relationship. The computers that make their file systems or directories and other resources available for remote access are called servers. The act of making file systems available is called exporting. The computers (or the processes they run) that use a server's resources are considered clients. Once a client mounts a file system that a server exports, the client can access the individual server files (access to exported directories can be restricted to specific clients).

The following is a list of the installp images that you have to install:

- bos.net.nfs.client
- bos.rte.filesystem

After installing the images, you need to start the NFS daemons. You can use the `mknfs` command that is located in /usr/sbin. The following is a list of the options that you can use:

- `mknfs -N`: - This starts the daemons.
- `mknfs -I`: - Include the lines necessary to start the daemons on the inittab; so, during the time that the system will be restarted, it will execute /etc/rc.nfs.
- `mknfs -B`: - Start the daemons and include the lines.

You can use the following command to see if the process is running:

```
# lssrc -a | grep nfs
 biod            nfs             10586   active
 nfsd            nfs             9300    active
 rpc.mountd      nfs             8268    active
 rpc.statd       nfs             8006    active
 rpc.lockd       nfs             10080   active
```

Now, you have to export a directory in your NFS server. We are going to use the directory of the Samba server to be the NFS server and the other to be the client.

You can use the command below to export the file system on your NFS server.

```
# mknfsexp -d /sambanfs -t rw -r samba2 -B
/sambanfs root=samba2
Exported /sambanfs
```

Here, `/sambanfs` is the file system that you want to export, and `samba2` is the hostname of the machine to which you want to give root access to this file system.

You can start to configure your NFS client server. Before you start to configure your NFS client, you have to make sure that you have installed the necessary images and that the daemons are running. The following is the procedure to configure the NFS client:

1. Create a mount point (/sambanfs)

   ```
   mkdir /sambanfs
   ```

2. Mount the remote file system in the mount point.

   ```
   mount samba1:/sambanfs /sambanfs
   ```

   Where `samba1` is the hostname of the NFS server.

Now, you can export the file system, `/sambanfs`, using the Samba server. This way, all the Samba servers are going to share the same file system; so, the Samba users can access the same files from all the Samba servers.

> **Note**
>
> If your Samba servers are runing on an SP, you can use the switch network to export the files. You can do this using the hostname associated to the switch interface on the NFS configuration instead of using the hostnames associated to the token ring or ethernet adapters.

You can use another solution to share the files between your Samba server. If you are running your samba server on an SP system, you can use DFS, VSD, RVSD, or GPFS. You can also use the concurrent logical volume, but you will find some limitations.

The Distributed File System (DFS) technology provides the ability to access and store data at remote sites similar to the techniques used with NFS. It extends the view of a local (and, therefore, size-limited) file system to a distributed file system of almost unlimited size located on several remote systems. A distributed file system has many advantages over a centralized system. These advantages include providing access to files from anywhere in the world, higher availability through replication, and providing system users the ability to access data from a nearly unlimited data space.

IBM Virtual Shared Disk (IBM VSD) is a distributed subsystem that allows application programs to execute on different SP nodes to access a raw logical volume as if it were local to each node. It also provides a device driver that allows application programs to stripe data across the physical disks in multiple virtual shared disks, thus, reducing I/O bottlenecks and hot spots. If you want to know more about VSD, you can access the following Web site:

`http://www.rs6000.ibm.com/resource/technology/sp_papers/vsd.html`

The Recoverable Virtual Shared Disk (RVSD) software provides high availability by recovering the IBM VSD software on a backup node and by taking over the shared data that is installed on twin-tailed disks. When a node failure occurs, the backup node takes over the primary node. The volume group is varied on, and the virtual shared disk is available and active again. No human intervention is needed to recover from the failure. If you want to know more about RVSD, you can access the following Web site:

`http://www.rs6000.ibm.com/resource/aix_resource/sp_books/rvsd/index.html`

The General Parallel File System (GPFS) is designed to provide a common file system for data shared among the nodes of the SP. This goal can be achieved using distributed file systems, such as NFS, but this often provides less performance and reliability than SP users require. GPFS provides the universal access that SP applications need with good performance and reliability characteristics. If you want to know more about GPFS, you can access the following Web site:

`http://www.rs6000.ibm.com/resource/aix_resource/sp_books/gpfs/`

The concurrent access volume group is a volume group that can be accessed from more than one host system simultaneously; therefore, it is called concurrent access. If you want to configure a concurrent access volume group, you need to instal the HACMP/CRM product (High Availability Cluster Multi-Processing for AIX, Concurrent Resource Manager feature). The following is a list of the limitations:

- Only some external disk subsystems are supported.
- A large VGDA format is not supported on the concurrent volume group.
- JFS is not supported on the concurrent access volume groups.
- Mirror Write Consistency Checking (MWCC) should be disabled on the concurrent access volume group.
- Bad block relocation should be disabled on the concurrent access volume groups.

If you want to know more about concurrent logical volumes, you can refer to Chapter 4 of the redbook, *AIX Logical Volume Manager, from A to Z: Introduction and Concepts*.

6.5 Disk quotas

The disk quota system allows system administrators to control the number of files and data blocks that can be allocated to users or groups.

Samba has experimental quota support available. It is an option that you can choose at compile-time, but all it does is return different values for the size of the disk share and the amount of space free. This option can be useful in preventing confusion among the users and the Windows software. The place to start is by enabling quotas on the file system itself.

Disk quotas are implemented at the file system level in AIX. It is not Samba's responsibility to limit a user's disk usage. In this section we will describe how you can implement the disk quota on AIX.

6.5.1 Understanding disk quotas

The disk quota system is based on the Berkeley Disk Quota System and provides an effective way to control the use of disk space. The quota system can be defined for individual users or groups and is maintained for each journaled file system.

The disk quota system establishes limits based on three parameters that can be changed with the `edquota` command:

- User or group soft limits
- Uses or group hard limits
- Quota grace period

The soft limit defines the number of 1 KB disk blocks or files below which the user should remain. The hard limit defines the maximum amount of disk blocks or files the user can accumulate under the established disk quotas. The quota grace period allows the user to exceed the soft limit for a short period of time (the default value is one week). If the user fails to reduce usage below the soft limit during the specified time, the system will interpret the soft limit as the maximum allocation allowed, and no further storage will be allocated to the user. The user can reset this condition by removing enough files to reduce usage below the soft limit.

The disk quota system tracks user and group quotas in the quota.user and quota.group files that reside in the root directories of file systems enabled with quotas. These files are created with the `quotacheck` and `edquota` commands and are readable with the `quota` commands.

6.5.2 Prerequisites

You need to have installed the fileset bos.sysmgt.quota. This fileset provides the commands that enable you to establish, maintain, and report file system quotas. You can use the command, shown in the following screen, to verify if you have installed this fileset.

```
# lslpp -L bos.sysmgt.quota
  Fileset                      Level  State  Description
  ----------------------------------------------------------------------------
  bos.sysmgt.quota           4.3.3.0    C    Filesystem Quota Commands


State Codes:
 A -- Applied.
 B -- Broken.
 C -- Committed.
 O -- Obsolete.  (partially migrated to newer version)
 ? -- Inconsistent State...Run lppchk -v.
```

If you do not have this fileset installed, you can use the following command to install it:

```
installp -aX -d/dev/cd0/usr/sys/inst.images bos.sysmgt.quota
```

Where `/dev/cd0/usr/sys/inst.images` is the location of the fileset.

6.5.3 Procedure

Perform the following steps to set up quotas on your specific file system:

1. Determine which file systems require a quota. The disk quota can only be used with a journaled file system.
2. Use the `chfs` command to include the userquota and groupquota configuration attributes in the /etc/filesystems file. The following example enables both user and group quotas on the /test file system.

   ```
   chfs -a “quota = userquota,groupquota” /test
   ```

   You should see the corresponding entry in /etc/filesystems as shown in the following screen:

```
/test:
        dev             = /dev/lv00
        vfs             = jfs
        log             = /dev/hd8
        mount           = true
        options         = rw
        account         = false
        quota           = userquota,groupquota
```

3. Make sure that you have mounted the file system.

4. Set the desired quota limits for each user or group. You can use the `edquota` command to create each user or group’s soft and hard limits for allowable disk space and maximum number of files.

   The following example shows how you can enter a quota limit for the user, user1.

   ```
   edquota user1
   ```

   You will see a screen like the following:

   ```
   Quotas for user user1:
   /test: blocks in use: 0, limits (soft = 0, hard = 0)
          inodes in use: 0, limits (soft = 0, hard = 0)
   ```

   You have to enter the soft and hard values for the blocks and inodes. You can see the following screen to understand the meaning of each field:

   ```
   Quotas for user user1:
   /test: blocks in use: 27, limits (soft = 100, hard = 150)
          inodes in use: 30, limits (soft = 200, hard = 250)
   ```

   This user has used 27 KB of disk space. During the grace period, he or she can use 150 KB of disk space, and after the grace period only 100 KB. The user has 30 files but with a limit of 200 files during the grace period and 250 after the grace period.

   You can copy the quotas established for one user to another. The following is the command to copy the quota from `user1` to `user2`:

   ```
   edquota -p user1 user2
   ```

5. You can use the `edquota` command to add a quota for a group. The following is the command to add a quota for a group called `quotagrp`:

   ```
   edquota -g quotagrp
   ```

6. Enable the quota system with the `quotaon` command. The `quotaon` command enables quotas for a specified file system or for all file systems with a quota defined if you use the `-a` flag.

   ```
   quotaon /test
   ```

6.5.4 Additional commands

Now that you have finished the configuration process of the disk quota, you can use some additional commands to help you perform the administrative tasks.

The quota command displays disk usage and quotas. By default (or with the -u flag), only user quotas are displayed. The quota command reports the quotas of all file systems listed in the /etc/filesystems file. If the quota command exits with a non-zero status, one or more file systems are over quota. A root user may use the -u flag with the optional user parameter to view the limits of other users. Users without root user authority can view the limits of groups of which they are members by using the -g flag with the optional Group parameter. The following screen shows an example of using the quota command as a user and as root.

```
# su - user1
$ quota
Disk quotas for user user1 (uid 203):
     Filesystem  blocks   quota   limit   grace   files   quota   limit   grace
          /test       4     100     150               1     200     250
$exit
# quota -u user1
Disk quotas for user user1 (uid 203):
     Filesystem  blocks   quota   limit   grace   files   quota   limit   grace
          /test       4     100     150               1     200     250
```

The quotacheck command examines a file system, builds a table of current disk usage, and compares the information in the table to that recorded in the file system's disk quota file. If any inconsistencies are detected, the quota files are updated. If an active file system is checked, the current system copy of the incorrect quotas is updated as well.

The quotacheck command normally operates silently. If the -v flag is specified, the quotacheck command reports discrepancies between the calculated and recorded disk quotas.

The quotacheck command expects each file system to contain the quota.user and quota.group files located at the root of the associated file system. These default file names can be changed in the /etc/filesystems file. If these files do not exist, the quotacheck command creates them.

Note

Do not run the quotacheck command against an active file system. If the file system has any current activity, running the quotacheck command may result in incorrect disk usage information.

It is recommended to check and turn on quotas during system startup. To enable this check and to turn on quotas during system startup, add the following lines at the end of the /etc/rc file:

```
echo " Enabling filesystem quotas "
/usr/sbin/quotacheck -a
/usr/sbin/quotaon -a
```

Chapter 7. Sizing guidelines

Every system will reach a bottleneck at a certain level of performance. Some bottlenecks are easy to predict; for instance, a type of network cable can only transfer data up to its specified rate. Other bottlenecks are harder to predict, for example, interactions between client and server, such as file size and client activity.

In order to ahcieve good performance in your server, you need to size your server appropriately. Good performance in a computer system usually means that the system responds to user requests in an acceptable time. This can mean anything from microseconds in real-time systems to hours for very large numeric-intensive computing jobs.

You need to decide which configuration will be needed to fulfill these expectations. A detailed walkthrough of the design specification can give an estimate of what resources the target system would need to handle the planned transaction workload. All workloads are made of the following:

- CPU resources consumed
- Memory resources consumed
- I/O load
- Network load

By decomposing a given workload into these basic elements, it is possible to estimate the CPU, main memory, disk, and network resources needed to fulfill the response time requirements.

For most servers, the CPUs are rarely the bottleneck, but you can reach a bottleneck if you connect hundreds of users at the same time. You will find some useful information to answer this question in the following sections.

It is harder to estimate how many I/O operations per second to expect in your server. The I/O operations depend, basically, on client activity and file size. The hard disks will always bottleneck at a specific number of I/O operations per second.

Network performance is dependent on the type of network, such as token ring, Ethernet, FDDI, or ATM, but it is also highly dependent on the application, the frequency of data transfers, the protocol, and the amount of data that is transferred through the network as well as on the design of the entire network.

One basic thing to understand is that you should never expect network traffic to be as fast as the indicated throughput of the adapter. Throughput can be defined as the amount of data exchanged between systems over a given time interval. In a real production environment, individual components within the larger network can also affect throughput. In fact, the slowest component within a network is the bottleneck that determines that network's maximum throughput.

Since our resources and time were limited, we decided to focus our experimentation on activities very specific to Samba. If you are looking for a better understanding of RS/6000 sizing, refer to the redbook, *Understanding IBM RS/6000 Performance and Sizing*, SG24-4810.

We have tried to find a reasonable answer to three main factors of the sizing, CPU, memory and network.

7.1 Practical experimentation

Since our lab had neither all of the equipment required to connect thousands of users nor hundred of users to enter commands on the keyboard, we had to find an alternate way to simulate users' connections. What we did was to slightly modify the smbclient program part of the Samba distribution. We have instrumented it with time measurement routines and the capability to fork a given number of client spread over some time. The initial idea of the test was to estimate the maximum number of operations that could be achieved by the RS/6000 server; so, we would have started a thousand requests at the same time and observe the behavior of the system. The first result showed that this was not convincing and may be a bit far from reality. Then, the second version of our test allowed us to start the same thousand requests, evenly spread over one minute, which seems to better reflect reality. We then developed the following eight sets of scripts:

1. This test simulates a given number of clients that connect to the server within a minute, wait some time, then disconnect from the server. The reason for that delay, is that disconnection also uses some CPU and we don't want to confuse the CPU used by the connection process with the one used by the disconnection process. This test has two sections:
    a. Local authentication done by the Samba server using the smbpasswd file.
    b. Remote authentication using a Microsoft Windows NT Primary Domain Controller.

2. This test simulates a given number of users connecting to the server, changing directories, and listing the files in the new directory.
3. This test simulates a given number of users connecting to the server, changing directories ten times, and listing the files in each directory. This test tries to simulate a browsing activity.
4. This test simulates a given number of users connecting to the server and getting a 10 KB file. The reason for such a small file is to measure the CPU associated with the retrieval of a file and must not be impacted by I/O or Network bottleneck.
5. This test simulates a given number of users connecting to the server and putting a 10 KB file. The reason for such a small file is to measure the CPU associated with the retrieval of a file and must not be impacted by I/O or Network bottleneck.
6. This test simulates a given number of users connecting to the server and printing a 10 KB file. The reason for such a small file is to measure the CPU associated with the retrieval of a file and must not be impacted by I/O or Network bottleneck. We have also created a dummy print queue because, afterwards, it was quite hard to distinguish between the CPU load from the Samba server, the print server, and the CPU. The time taken by a print job can vary enormously with the type of spool job. In this experiment, once the print job is in the print queue, we consider it done.
7. This test is a mix of the previous tests. We simulate a given number of users connecting to the server, browsing the directories, and putting and getting 10 KB files. This is an attempt to simulate some active users.
8. This test studies the transfer of a large file where I/O and network become the bottleneck. We simulate a given number of users transferring a 10 MB file from the client to the server.

Those tests have been conducted on a 43P-150, 43P-260, F50, and an S7A connected on an isolated 16 Mb Token Ring Network. Each time, the test script are launched from a remote RS/6000, and we also run the `vmstat` command on this client machine to make sure that it does not become the bottleneck of our experience.

7.1.1 Results

During these tests, we are recording the impact on the server using the `vmstat` commands. The results we are given now are the number of refused connections (when the Samba server becomes too busy, it refuses new connections), the time used to perform an operation (connection, browsing, get, put, and print file), as well as the average CPU load on the server during that operation.

7.1.2 The RS/6000 43P-150

The first machine tested is an RS/6000 43P-150. The machine used to simulate the clients is a 4-way F50.

7.1.2.1 Configuration

The machine was a uniprocessor 43p150 with a 375 Mhz 604e processor card. It has 512 MB of RAM, two 4.5 GB disks, the operating system being installed on the first disk. Our experience data are on the second disk (no mirrored no striped logical volumes). It also has a Token Ring adapter.

The version of AIX is 4.3.3, and we used Samba 2.0.6.

7.1.2.2 Results

Figure 79 shows the number of connections refused as the number of connections attempted increases.

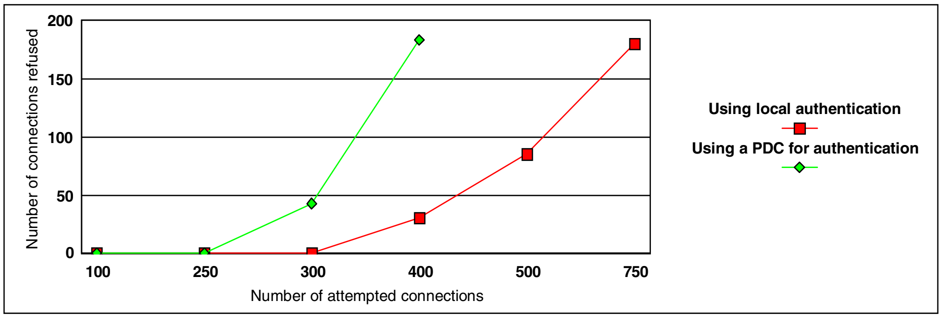


Figure 79. Number of refused connections

Figure 80 on page 171 shows the time it takes to connect to a server (as a function of the number of attempted connections) and the associated CPU load on the server.

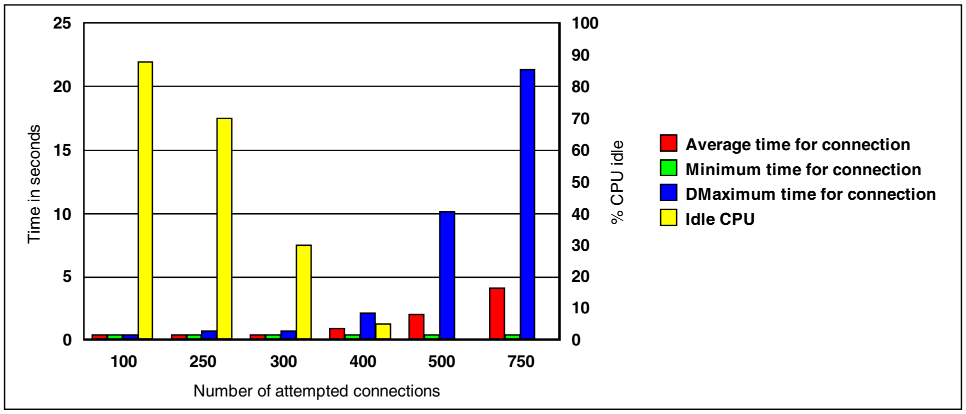


Figure 80. Time required per connection

Figure 81 shows the time it takes to connect to a server authenticating to a primary domain controller (as a function of the number of attempted connections) and the associated CPU load on the server.

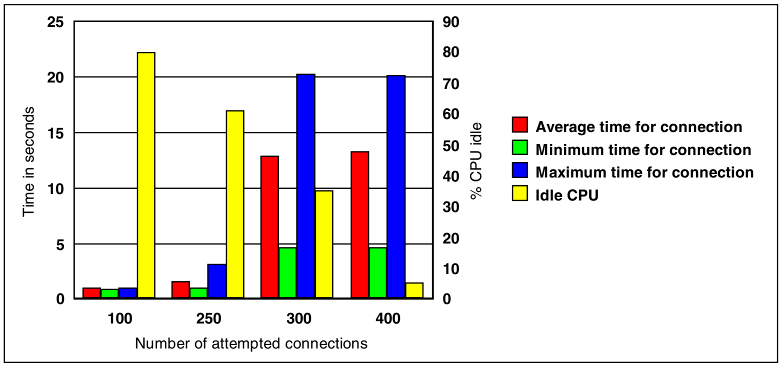


Figure 81. Time required per connection when authenticating to a PDC

Figure 82 on page 172 shows the time it takes to connect to a server and change directories (as a function of the number of attempted connections) and the associated CPU load on the server.

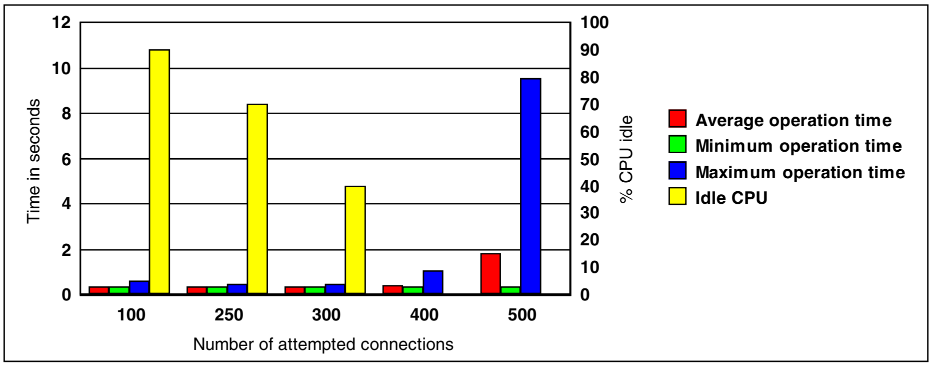


Figure 82. Time required to connect and change a directory

Figure 83 shows the time it takes to connect to a server and change ten time directories (as a function of the number of attempted connections) and the associated CPU load on the server.

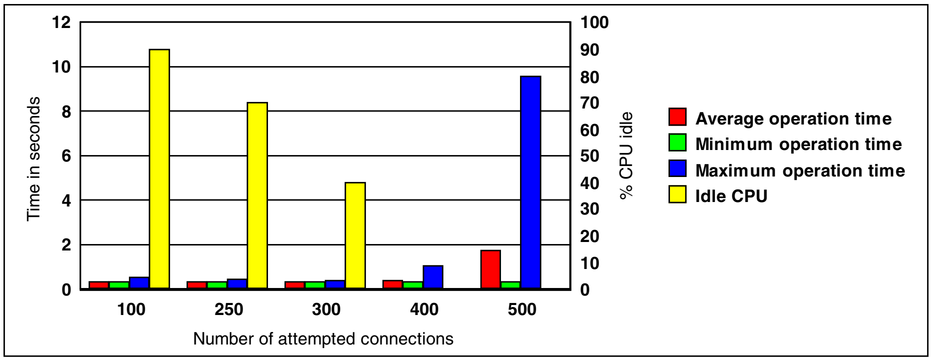


Figure 83. Time required to connect and browse a file

Figure 84 on page 173 shows the time it takes to connect to a server and get a 10 KB file (as a function of the number of attempted connections) and the associated CPU load on the server.

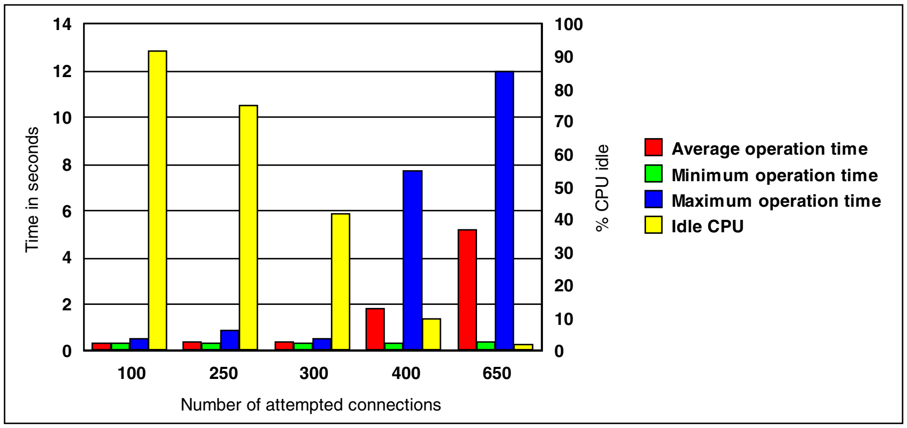


Figure 84. Time required to connect and get a 10 KB file

Figure 85 shows the time it takes to connect to a server and put a 10 KB file (as a function of the number of attempted connections) and the associated CPU load on the server.

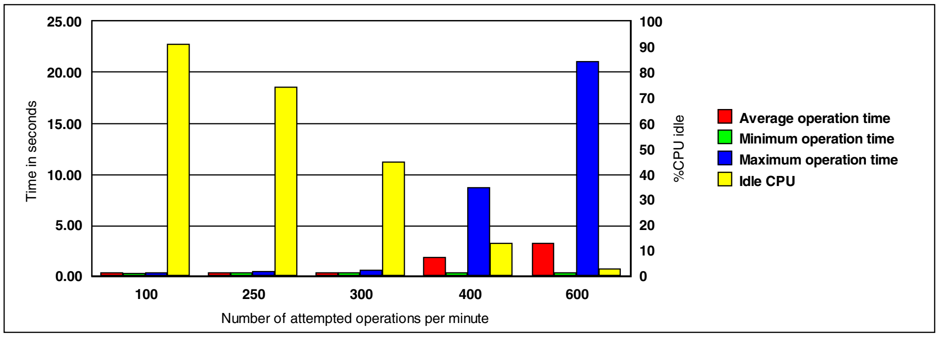


Figure 85. Time required to connect and put a 10 KB file

Figure 86 on page 174 shows the time it takes to connect to a server and print a 10 KB file (as a function of the number of attempted connections) and the associated CPU load on the server.

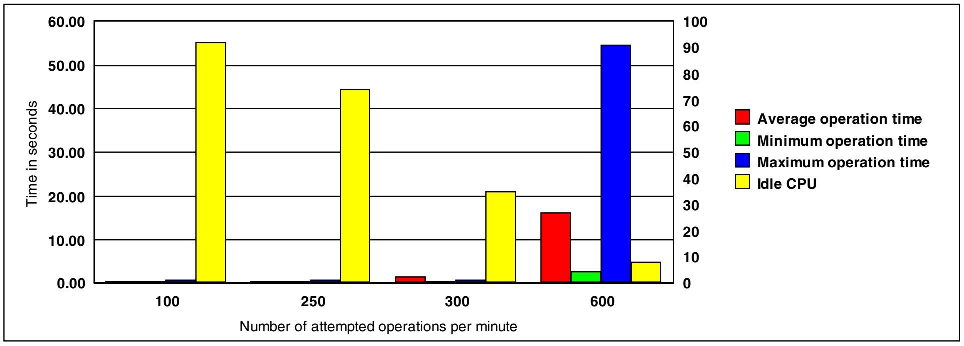


Figure 86. Time required to connect and print a 10 KB file

Figure 87 shows the time it takes to connect to a server and transfer a 10 MB file (as a function of the number of attempted connections) and the associated CPU load on the server. We use a line representation because of the large disparity of the results.

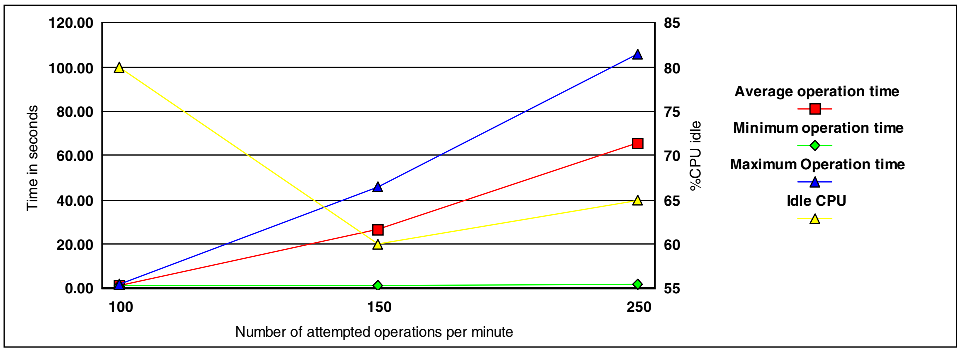


Figure 87. Time required to connect and transfer a 10 MB file

7.1.3 The RS/6000 43P-260

The first machine tested was an RS/6000 43P-260. The machine used to simulate the clients was a 4-way F50.

7.1.3.1 Configuration

The machine is a 2-way 43p260 with 200 Mhz POWER3 processors. It has 1 GB of RAM, two 4.5 GB disks, the operating system being installed on the first disk, and our experience data are on the second disk (no mirrored or striped logical volumes). It also has a Token Ring adapter.

The version of AIX was 4.3.3 and we used Samba 2.0.6.

7.1.3.2 Results

Figure 88 shows the number of connections refused as the number of connections attempted increases.

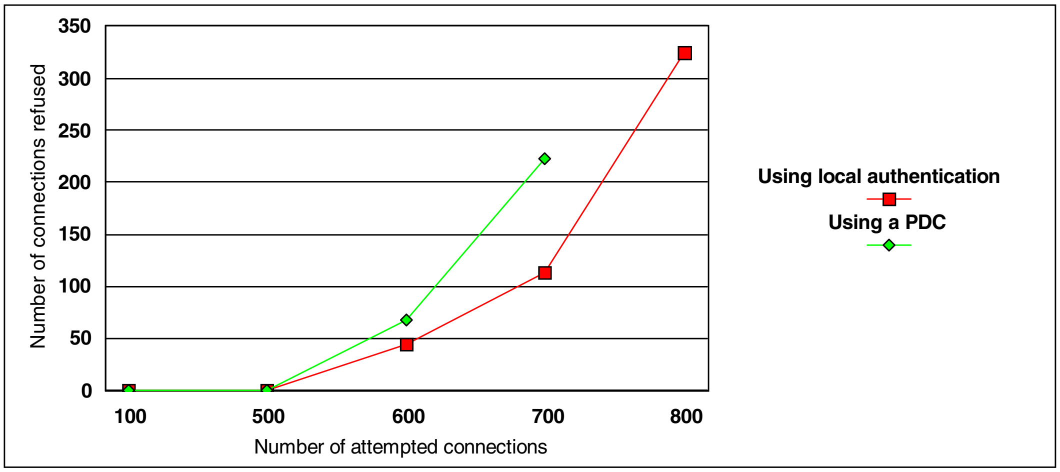


Figure 88. Number of refused connections

Figure 89 shows the time it takes to connect to a server (as a function of the number of attempted connections) and the associated CPU load on the server.

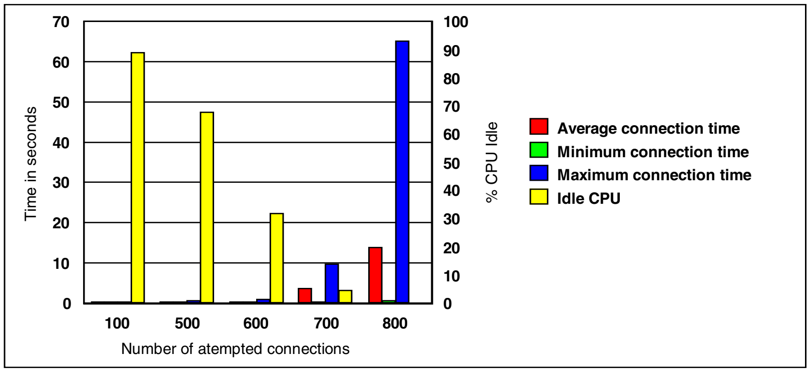


Figure 89. Time required per connection

Figure 90 on page 176 shows the time it takes to connect to a server authenticating to a primary domain controller (as a function of the number of attempted connections) and the associated CPU load on the server.

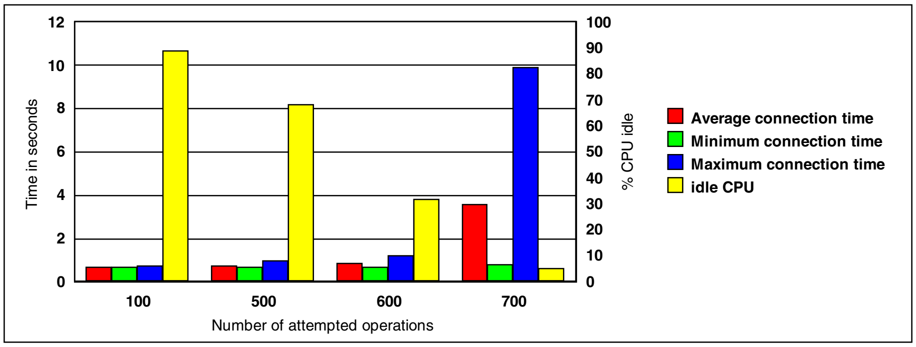


Figure 90. Time required per connection when authenticating to a PDC

Figure 91 shows the time it takes to connect to a server and change a directory (as a function of the number of attempted connections) and the associated CPU load on the server.

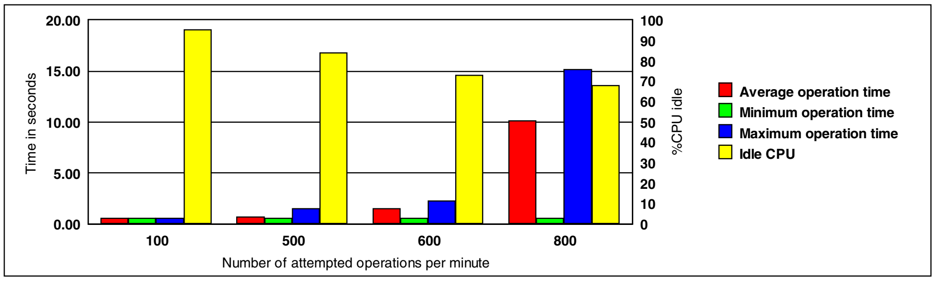


Figure 91. Time required to connect and change a directory

Figure 92 on page 177 shows the time it takes to connect to a server and change ten time directories (as a function of the number of attempted connections) and the associated CPU load on the server.

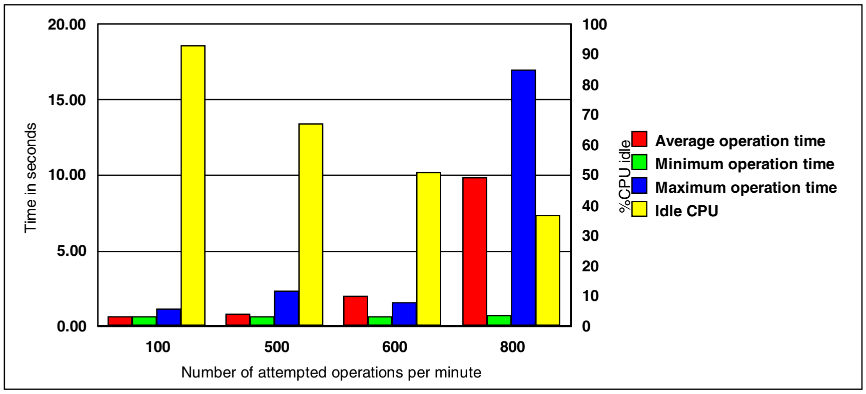


Figure 92. Time required to connect and browse a file

Figure 93 shows the time it takes to connect to a server and get a 10 KB file (as a function of the number of attempted connections) and the associated CPU load on the server.

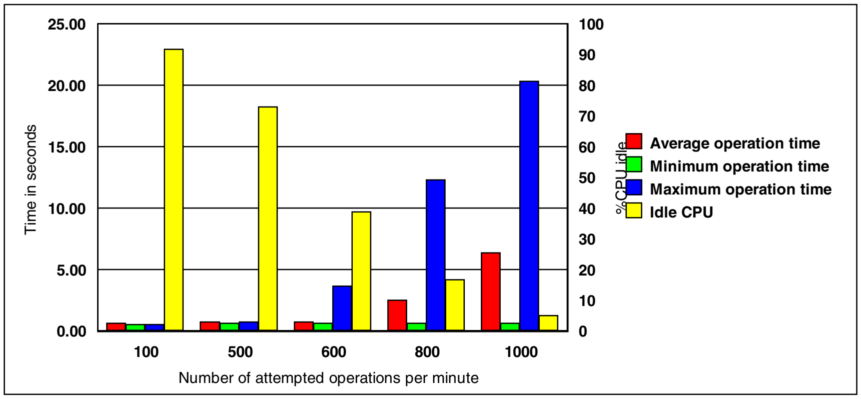


Figure 93. Time required to connect and get a 10 KB file

Figure 94 on page 178 shows the time it takes to connect to a server and put a 10 KB file (as a function of the number of attempted connections) and the associated CPU load on the server.

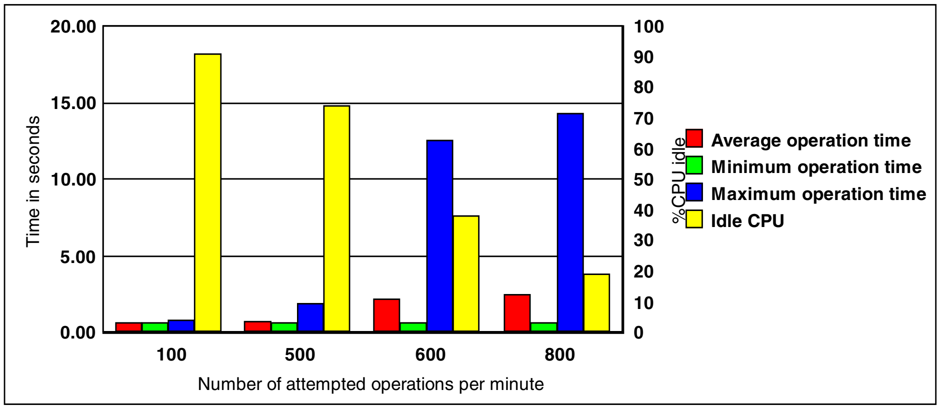


Figure 94. Time required to connect and put a 10 KB file

Figure 95 shows the time it takes to connect to a server and print a 10 KB file (as a function of the number of attempted connections) and the associated CPU load on the server.

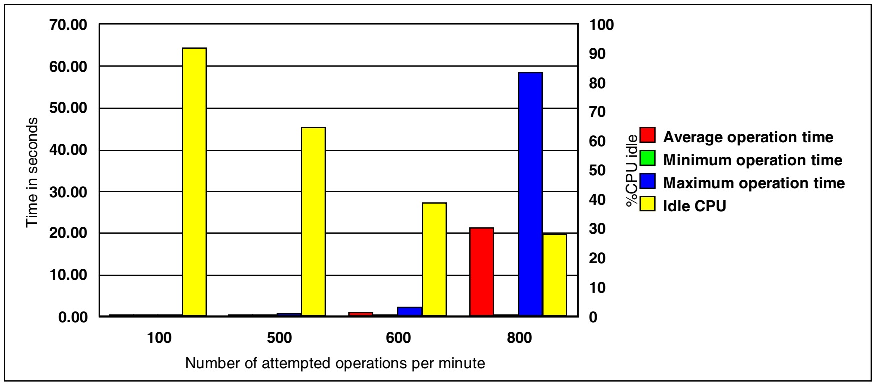


Figure 95. Time required to connect and print a 10 KB file

Figure 96 on page 179 shows the time it takes to connect to a server and transfer a 10 MB file (as a function of the number of attempted connections) and the associated CPU load on the server. We use a line representation because of the large disparity of the results.

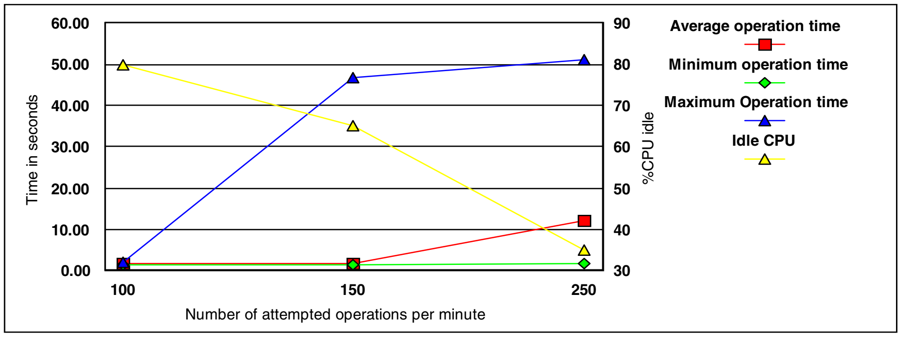


Figure 96. Time required to connect and transfer a 10 MB file

7.1.4 The RS/6000 4-way F50

The third machine tested was an RS/6000 F50. The machine used to simulate the clients was a 12-way S7A.

7.1.4.1 Configuration

The machine was a 4-way F50 with 332 Mhz 604e processors. It had 2 GB of RAM, two 4.5 GB disks, the operating system being installed on the first disk, and our experience data were on the second disk (no mirrored or striped logical volumes). It also has a Token Ring adapter.

The version of AIX is 4.3.3 and we use Samba 2.0.6.

7.1.4.2 Results

Figure 97 on page 180 shows the number of connections refused as the number of connections attempted increases.

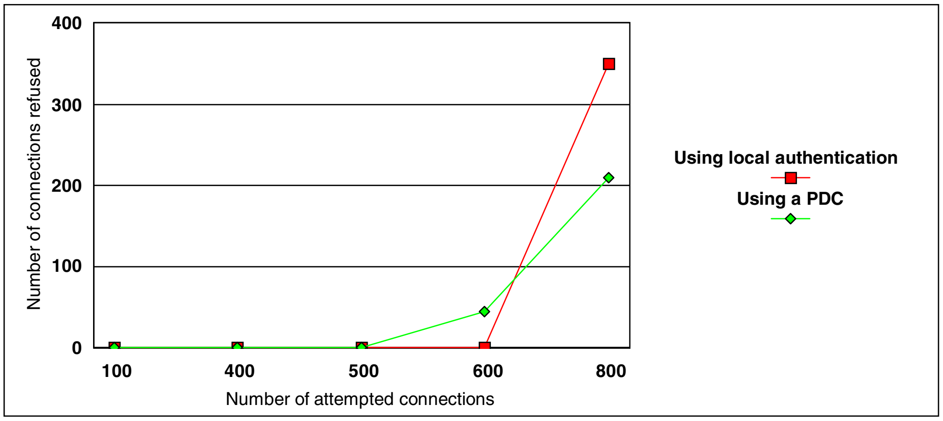


Figure 97. Number of refused connections

Figure 98 shows the time it takes to connect to a server (as a function of the number of attempted connections) and the associated CPU load on the server.

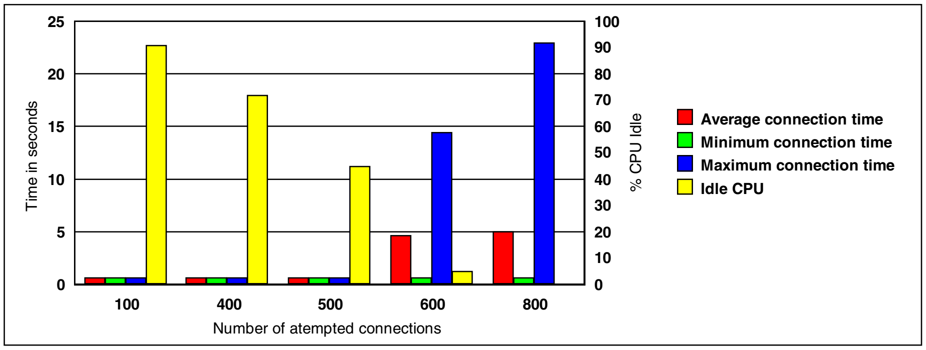


Figure 98. Time required per connection

Figure 99 on page 181 shows the time it takes to connect to a server authenticating to a primary domain controller (as a function of the number of attempted connections) and the associated CPU load on the server.

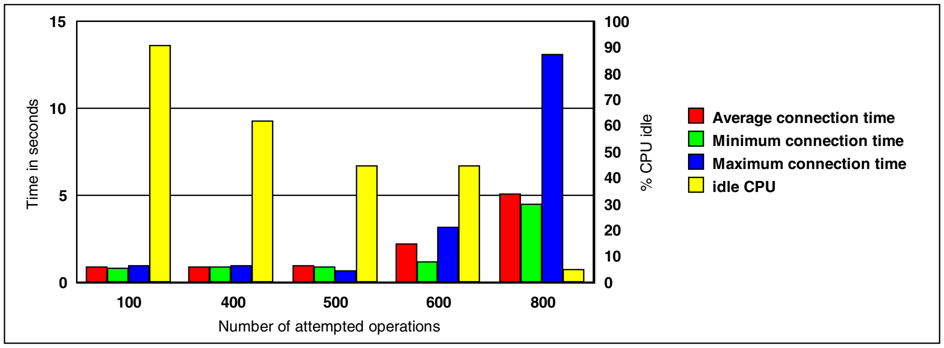


Figure 99. Time required per connection when authenticating to a PDC

Figure 100 shows the time it takes to connect to a server and change directories (as a function of the number of attempted connections) and the associated CPU load on the server.

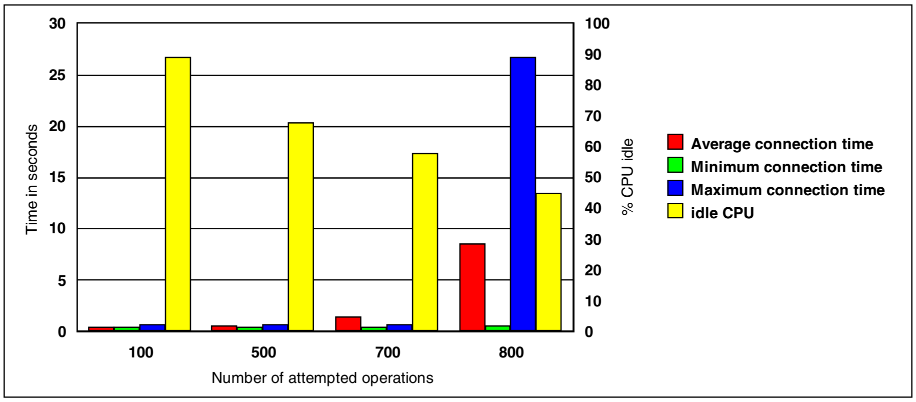


Figure 100. Time required to connect and change a directory

Figure 101 on page 182 shows the time it takes to connect to a server and change ten time directories (as a function of the number of attempted connections) and the associated CPU load on the server.

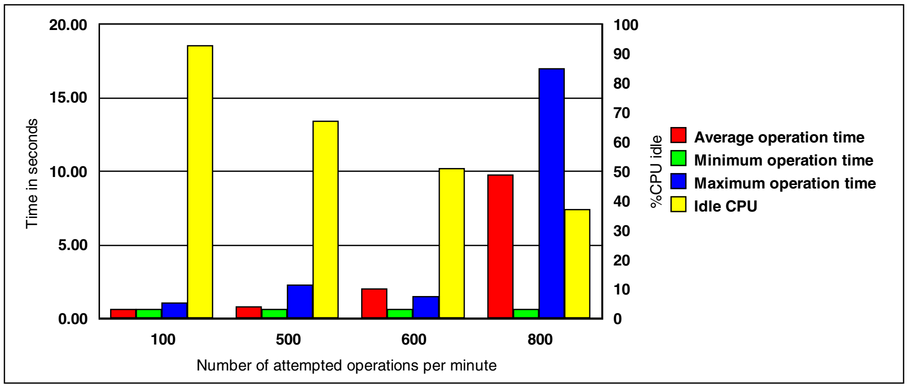


Figure 101. Time required to connect and browse a file

Figure 102 shows the time it takes to connect to a server and get a 10 KB file (as a function of the number of attempted connections) and the associated CPU load on the server.

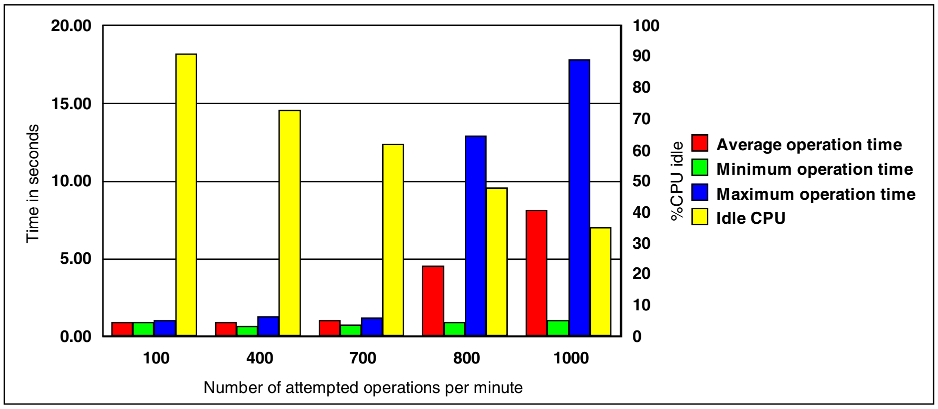


Figure 102. Time required to connect and get a 10 KB file

Figure 103 on page 183 shows the time it takes to connect to a server and put a 10 KB file (as a function of the number of attempted connections) and the associated CPU load on the server.

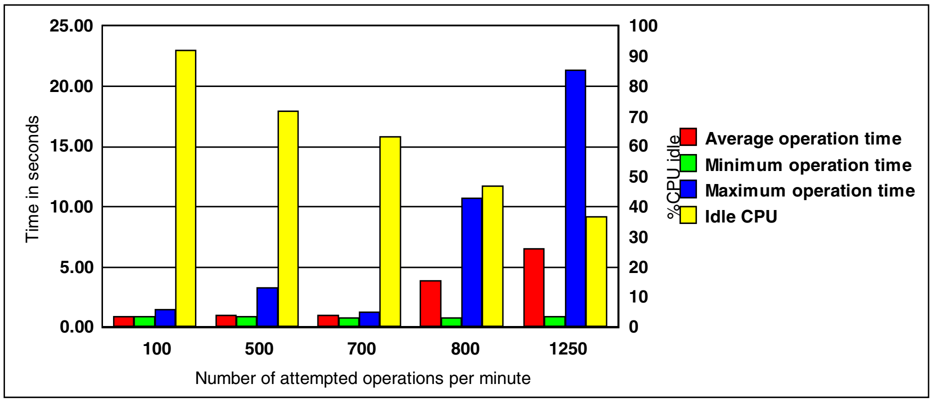


Figure 103. Time required to connect and put a 10 KB file

Figure 104 shows the time it takes to connect to a server and print a 10 KB file (as a function of the number of attempted connections) and the associated CPU load on the server.

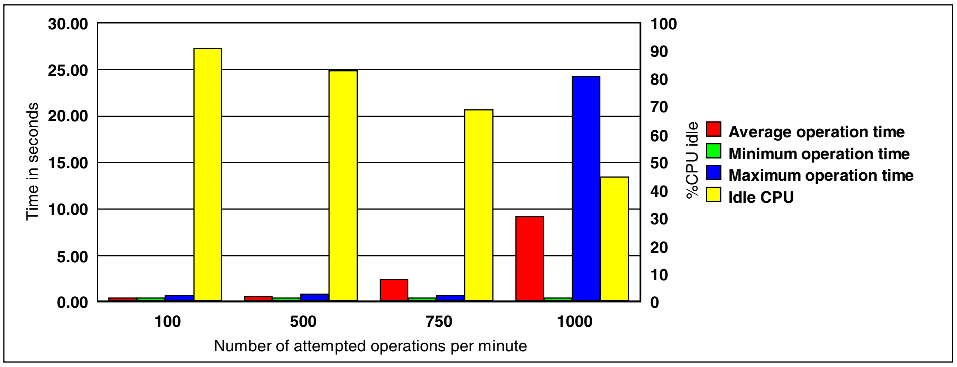


Figure 104. Time required to connect and print a 10 KB file

Figure 105 on page 184 shows the time it takes to connect to a server and transfer a 10 MB file (as a function of the number of attempted connections) and the associated CPU load on the server. We use a line representation because of the large disparity of the results.

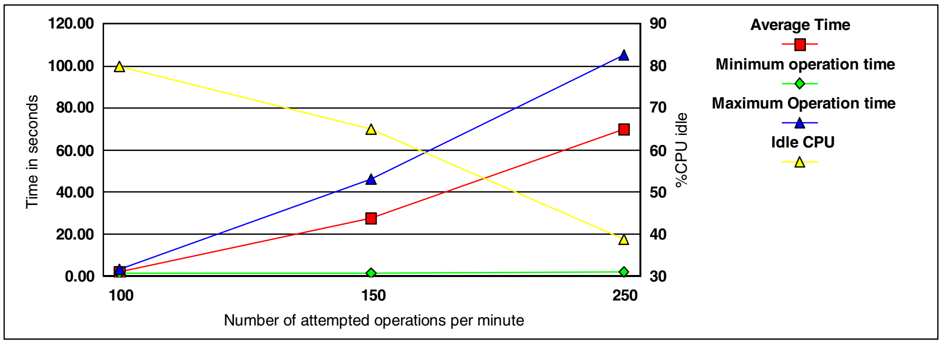


Figure 105. Time required to connect and transfer a 10 MB file

7.1.5 The RS/6000 12-way S7A

The last machine we tested was a 12-way RS/6000 S7A. That experiment was a bit different since the system had only 1 GB of memory and could not accept two many connections, and we did not have any machine powerful enough to act as the client; so, we used three systems as the client: The F50, the 43P260, and a J50 (a 4-way 120 MHz 604 processor), and we spread the load over 30 seconds instead of one minute as we had done previously.

7.1.5.1 Configuration

The machine is a 12-way S7A with 262 MhzRS64 II processors. It has 1 GB of RAM, 11 4.5 GB disks. The operating system being installed on the first disk and our experience data are on the other disks (no mirrored or striped logical volumes). It also has a Token Ring adapter.

The version of AIX is 4.3.3 and we use Samba 2.0.6.

7.1.5.2 Results

Figure 106 on page 185 the number of connections refused as the number of connections attempted increases.

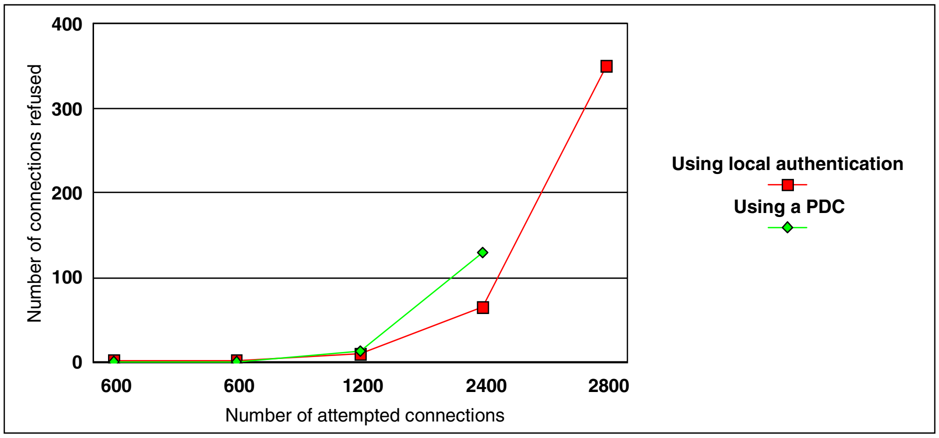


Figure 106. Number of refused connections

Figure 107 shows the time it takes to connect to a server (as a function of the number of attempted connections) and the associated CPU load on the server.

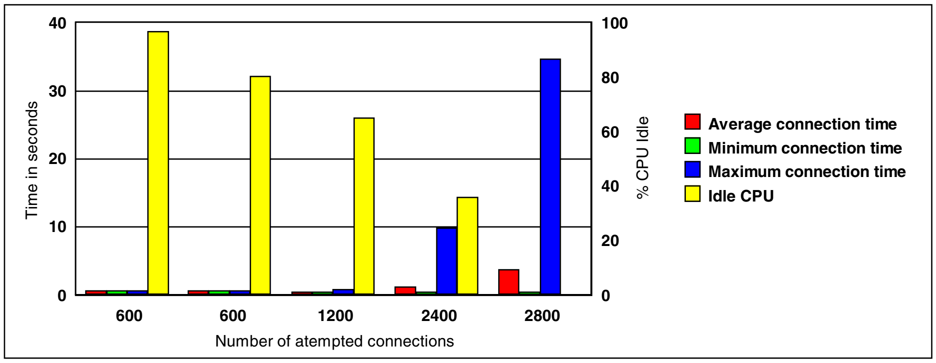


Figure 107. Time required per connection

Figure 108 on page 186 shows the time it takes to connect to a server authenticating to a primary domain controller (as a function of the number of attempted connections) and the associated CPU load on the server.

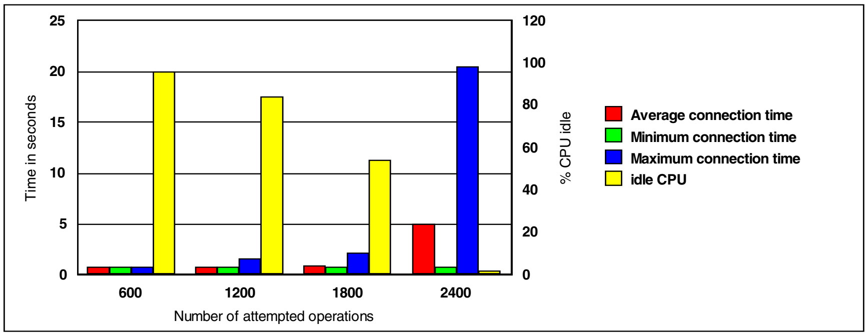


Figure 108. Time required per connection when authenticating to a PDC

Figure 109 shows the time it takes to connect to a server and change directories (as a function of the number of attempted connections) and the associated CPU load on the server.

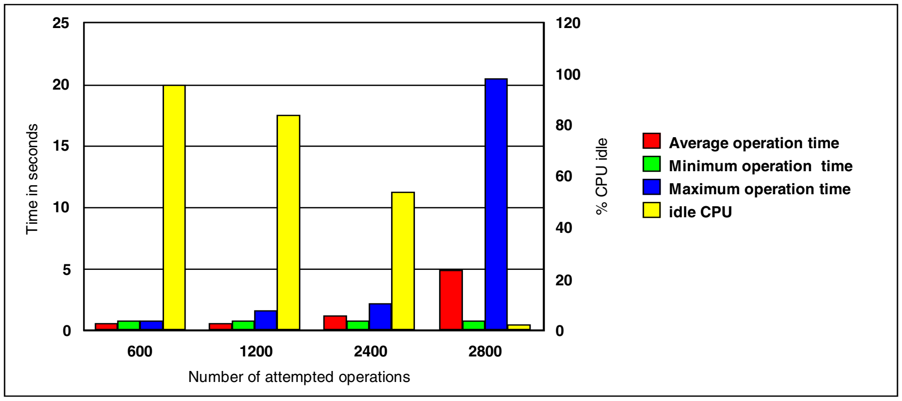


Figure 109. Time required to connect and change a directory

Figure 110 on page 187 shows the time it takes to connect to a server and change ten time directories (as a function of the number of attempted connections) and the associated CPU load on the server.

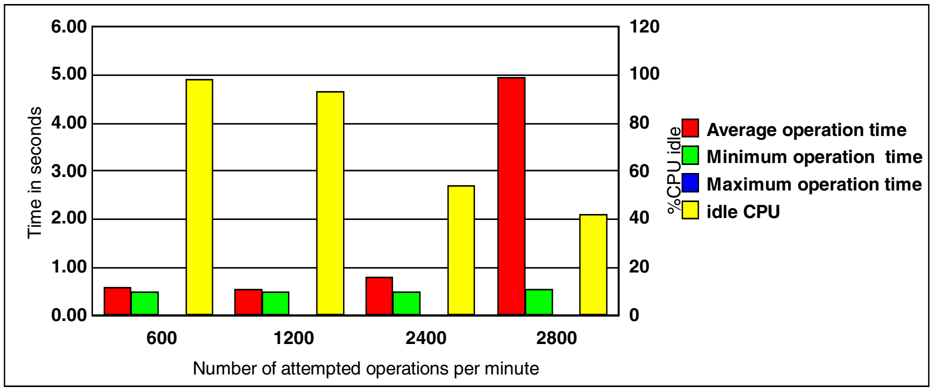


Figure 110. Time required to connect and browse a file

Figure 111 shows the time it takes to connect to a server and get a 10 KB file (as a function of the number of attempted connections) and the associated CPU load on the server.

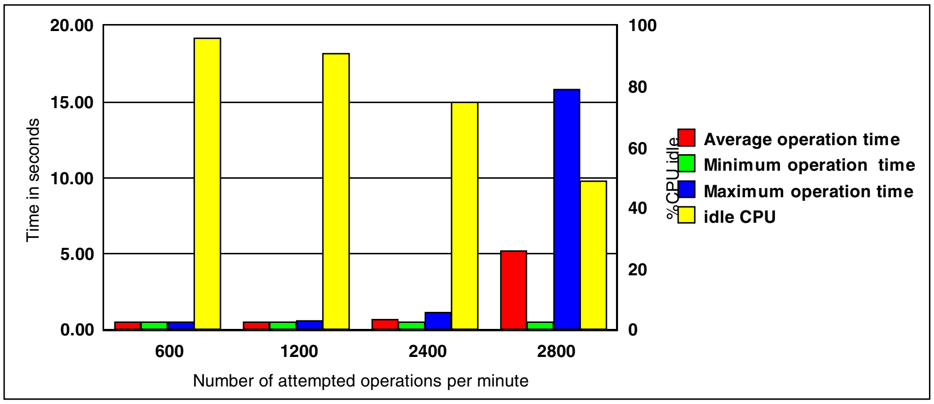


Figure 111. Time required to connect and get a 10 KB file

Figure 112 on page 188 shows the time it takes to connect to a server and put a 10 KB file (as a function of the number of attempted connections) and the associated CPU load on the server.

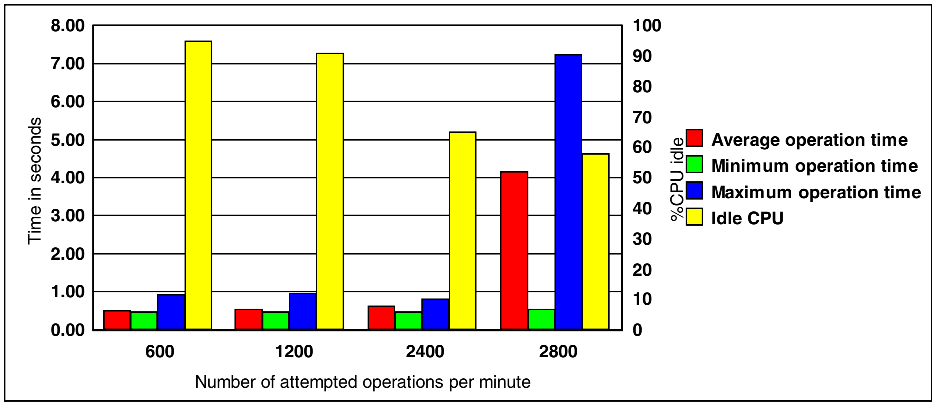


Figure 112. Time required to connect and put a 10 KB file

Figure 113 shows the time it takes to connect to a server and print a 10 KB file (as a function of the number of attempted connections) and the associated CPU load on the server.

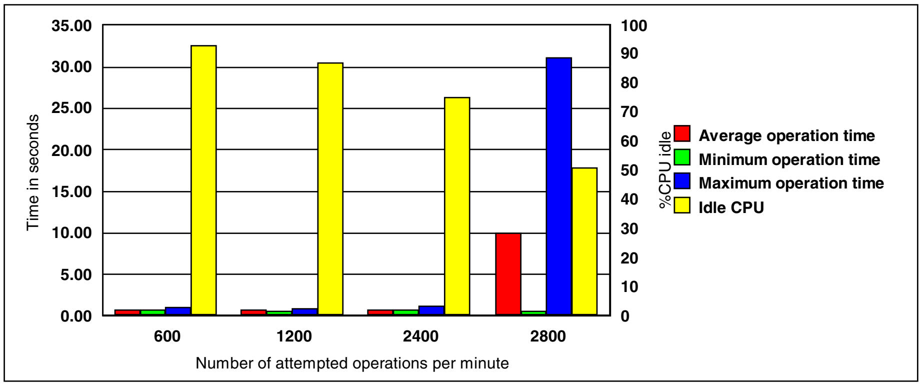


Figure 113. Time required to connect and print a 10 KB file

Figure 114 on page 189 shows the time it takes to connect to a server and transfer a 10 MB file (as a function of the number of attempted connections) and the associated CPU load on the server. We use a line representation because of the large disparity of the results.

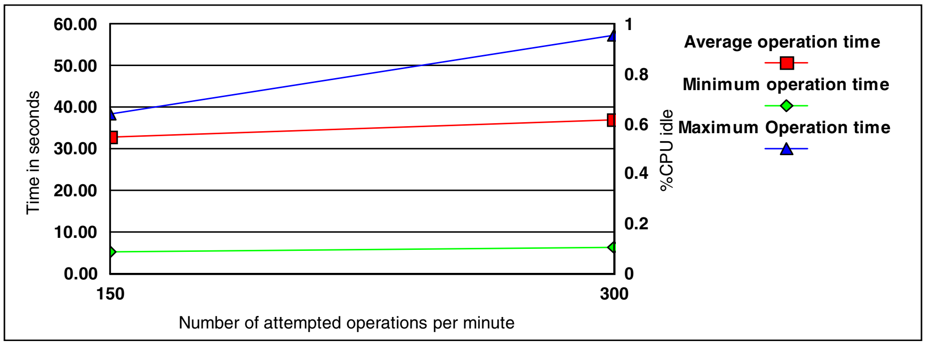


Figure 114. Time required to connect and transfer a 10 MB file

7.1.6 Conclusion

At the end of these tests, there were some conclusions that could be extracted from these numbers. Let us start with the easy ones.

7.1.6.1 Memory sizing

The reading of the result of the `vmstat` commands confirms the developers' design. To every connecting user, a new thread and process are associated. The memory requirement for these entities is about 512 KB. Whether the user is active or not does not change this value. If the user is not active, this memory will likely be swapped out. On top of that, you will have to consider the memory for the operating system, any additional application you might run on the server, and the memory mapping for the files used on the system.

7.1.6.2 Network sizing

Sizing the network is usually a complex task; the only goal we had during this experimentation was to make sure that using Samba would not add any hidden overhead to the file transfers. The connection, authentication, and change directories commands are very lightweight and do not have a big impact on the network. The transfer rate observed during the get and put operations for big files show that we reached the nominal bandwidth of the network; so, the choice of network must be made in the function of the expected network traffic. Samba does not add any overhead.

7.1.6.3 CPU sizing

It is not easy to define an average user in a manner that would be compatible with any type of environment; so, we decided to run elementary tasks, and, after that, sizing the system would be based on how many of those tasks were run by the users of a specific environment. The heaviest operation, in terms of CPU, is the login-authenticating part. That is where we saw the limitation with the percentage of idle CPU being 0 percent and having a system that would no longer respond. Table 7 gives the maximum number of users that can connect within one minute for each of the systems tested. Of course, the maximum number of users for the system will be limited by the total amount of CPU. For example, on a 43P150 with 1 GB of memory, the maximum number of users that can connect within a minute is 500, but, if those users connect within a longer period, you can have 1700 users logged (that is, 1 GB of memory - 150 MB for the operating system and 512 KB of memory per user) before you start paging.

Table 7. Maximum number of users connecting within one minute

43P150	43P260	F50	S70
400	550	650	2800

The login/authenticating step is the heaviest; the other steps studied during our test never caused the system to be 100 percent full, but, once again, the tests were designed to be low I/O oriented. Once again, for a complete approach to system sizing, refer to the redbook, *Understanding IBM RS/6000 Performance and Sizing*, SG24-4810.

At the time this book is being written, there is another series of benchmarks being run by the AIX performance group using the Netbench Version 6 application. The results of these tests will be published as a white paper, and you will be able to find a copy at the following Web site:

`http://www.redbooks.ibm.com/portals/rs6000`

Appendix A. Troubleshooting

This appendix describes the basic tools for locating problems with Samba, clients, and SMB/CIFS protocols and how to narrow them down.

A.1 Protocol levels

It is hard to define, in a very strict way, how to find the problems in a domain as large as the combination of the SMB and TCP/IP protocols. The following sections provide some steps and hints you should not forget when troubleshooting the SMB protocol.

The TCP/IP protocol is divided into separate independent levels. This architecture helps us because, normally, we only have a problem in one level and must locate it. Here is a simplified version of these levels that can help you locate the problem. You should try to locate the lowest network level with the problem. If you have, for example, a problem with name resolution, access to the shares will probably not work.

- **TCP/IP protocols**
  - **Address resolution** - This is the conversion from the hardware network address to the IP address and back. The utilities are arp and ping.
  - **Routing** - This is a mechanism for transferring traffic (packets) from one network to another, that is, out of your local network and back. The utilities are traceroute, route, ping, netstat, and tracert.
  - **Name resolution** - This is the conversion from the domain name to the IP address. The utilities are nslookup and host.
- **SMB protocols**
  - **Name resolution** - This is the conversion from the SMB name to the IP address. The utility is nbtstat.
  - **Browsing** - This is the function on the SMB network that provides a list of accessible computers and resources to the clients. The utilities are browstat and smbclient.
  - **Authentication** - This is the verification of the client on the SMB server.
  - **Access** - This is the access of the client to the shared resources.
  - **Netlogon** - This is the network logon feature of the SMB server.

A.2 Generic TCP/IP utilities

If you know your network organization, use the following tools to check the status of the TCP/IP level of the network. If you do not know the network organization, use the same tools to find it. These utilities are available on AIX and also on Windows NT. Some of them may be missing on the Windows 95 system. These utilities are:

ipconfig This shows the IP configuration on Windows NT machines.

ping This checks the IP connectivity. Try to ping to localhost (127.0.0.1), local IP address, gateway, and remote computer. Try it with computer name and IP address.

traceroute This checks the route from one computer in a TCP/IP network to another (use tracert on client).

route This prints out the routing table. You can also add and delete routes.

netstat This shows the aspects of the status of the network, such as routing table, port allocation, and statistics.

nslookup This checks the Domain Name Service (DNS) - TCP/IP name resolution. You can find IP address from the computer name and vice versa.

arp This shows and modifies the table for IP address to adapter address translation.

Try to determine if the problem is only one computer.

A.3 Troubleshooting utilities on Windows NT

This section describes Windows NT tools for TCP/IP and SMB diagnostics.

A.3.1 TCP/IP configuration

The TCP/IP configuration of the Windows NT system can be obtained with the `ipconfig` command. You can use the /all switch to see detailed information about IP address, netmask, gateway address, and so forth.

```
Windows NT IP Configuration

        Host Name . . . . . . . . . : lv3030b.itsc.austin.ibm.com
        DNS Servers . . . . . . . . : 9.3.240.2
        Node Type . . . . . . . . . : Hybrid
        NetBIOS Scope ID. . . . . . :
        IP Routing Enabled. . . . . : No
        WINS Proxy Enabled. . . . . : No
        NetBIOS Resolution Uses DNS : Yes

Token Ring adapter Ibmtok51:

        Description . . . . . . . . : Ibm Token Ring Network Card for PC I/O bus.
        Physical Address. . . . . . : 00-06-29-68-8B-2E
        DHCP Enabled. . . . . . . . : Yes
        IP Address. . . . . . . . . : 9.3.240.123
        Subnet Mask . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . : 9.3.240.1
        DHCP Server . . . . . . . . : 9.3.240.2
        Primary WINS Server . . . . : 9.3.1.81
        Lease Obtained. . . . . . . : Monday, February 15, 1999 3:05:31 PM
        Lease Expires . . . . . . . : Tuesday, February 16, 1999 9:05:31 AM
```

You can use the `winipcfg` command on Windows 95 systems to get similar information.

You can use other commands that can help you analyze the configuration, routing, DNS, and other TCP/IP-related problems, such as `hostname`, `ping`, `netstat`, `route`, `arp` (see Chapter A.2, “Generic TCP/IP utilities” on page 192).

You may try using Solving Basic TCP/IP Problems procedure at the following Web site: `http://support.microsoft.com/support/tshoot/nt4_tcp.asp`

A.3.2 NetBIOS over TCP/IP troubleshooting

When you want to analyze NetBIOS over TCP/IP configuration, you have different utilities to check your NetBIOS name resolution, routing, and browsing.

A.3.2.1 tracert

The `tracert` command is a route tracing utility similar to the trace utility in UNIX. It determines a route to a destination by sending ICMP echo packets with varying time-to-live values (TTL). You can use the following options:

-d IP addresses are not resolved to hostnames.

-h This defines the maximum number of hops to reach the destination.

-j This specifies loose source route along host-list.

-w This specifies the wait time for each reply.

The output shows the steps to reach the destination. Every line shows the hop number, three round-trip times for three attempts, and the hostname (or IP address) of the system that was reached in this hop. An asterisk (*) means that the attempt timed out.

```
C:\>tracert lv3030c

Tracing route to lv3030c.itsc.austin.ibm.com [9.3.187.213]
over a maximum of 30 hops:

  1    10 ms     *      <10 ms  itso240.itsc.austin.ibm.com [9.3.240.1]
  2   <10 ms   <10 ms   <10 ms  lv3030c.itsc.austin.ibm.com [9.3.187.213]

Trace complete.
```

A.3.2.2 nbtstat

This tool is used for troubleshooting NetBIOS name resolution. The name resolution on Windows NT client uses one of the following methods: Local cache lookup, WINS server, broadcast, DNS, LMHOSTS, or HOSTS lookup. nbtstat can help you analyze name resolution problems with the following options:

-n This lists local registered NetBIOS names.

```
C:\>nbtstat -n

Node IpAddress: [9.3.240.113] Scope Id: []

           NetBIOS Local Name Table

   Name              Type         Status
---------------------------------------------
AUSRES10       <00>  UNIQUE      Registered
ITSOAUSNT      <00>  GROUP       Registered
AUSRES10       <03>  UNIQUE      Registered
AUSRES10       <20>  UNIQUE      Registered
INet~Services  <1C>  GROUP       Registered
IS~AUSRES10....<00>  UNIQUE      Registered
ITSOAUSNT      <1E>  GROUP       Registered
```

-a, -A These list the remote computer’s name table (similar to what option -n does for a local computer).

-c This shows the content of the NetBIOS name cache.

-r This shows the name resolution and registration statistics and also names resolved by broadcast.

-R This clears the local cache and reloads it from the LMHOSTS file.

-s, -S These list the NetBIOS sessions. The first option will show NetBIOS names and the second one IP addresses.

```
C:\>nbtstat -S

                 NetBIOS Connection Table

Local Name             State    In/Out  Remote Host          Input   Output
----------------------------------------------------------------------------
LV3030B        <00>  Connected    Out   ITSONT00       <20>   105KB    105KB
LV3030B        <00>  Connected    Out   LV3030C        <20>    11KB      1KB
LV3030B        <03>  Listening
LV3030B              Connected    In    AUSRES10       <00>     2MB      1MB
ADMINISTRATOR  <03>  Listening
```

A.3.2.3 browstat

The *Microsoft Windows NT Server Resource Kit 4.0* includes the browstat utility, shich can be used for analyzing SMB network.

The browstat utility can show you browsers and the domain organization of a network. It is a command line utility. Some options of the command require a *transport* parameter. You can retrieve it with browstat status (this is part of the output):

```
Status for domain ITSOAUSNT on transport \Device\NetBT_Ibmtok51
...

Status for domain ITSOAUSNT on transport \Device\Nbf_Ibmtok51
...
```

You can see two transports in this example: `NetBF_Ibmtok51` and `Nbf_Ibmtok51`.

Browstat has the following options:

status [-V] [domain] This shows the status of the domain. The -V switch shows us extended information. You can see basic browsing and domain information on this sample output:

```
Status for domain ITSOAUSNT on transport \Device\NetBT_Ibmtok51
    Browsing is active on domain.
    Master browser name is: AUSRES05
        Master browser is running build 1381
    3 backup servers retrieved from master AUSRES05
        \\AUSRES05
        \\AUSRES08
        \\AUSRES06
    There are 85 servers in domain ITSOAUSNT on transport \Device\NetBT_Ibmtok51
    There are 32 domains in domain ITSOAUSNT on transport \Device\NetBT_Ibmtok51

Status for domain ITSOAUSNT on transport \Device\Nbf_Ibmtok51
    Browsing is active on domain.
    Master browser name is: AUSRES10
        Master browser is running build 1381
    3 backup servers retrieved from master AUSRES10
        \\AUSRES03
        \\AUSRES11
        \\AUSRES10
    There are 42 servers in domain ITSOAUSNT on transport \Device\Nbf_Ibmtok51
    There are 2 domains in domain ITSOAUSNT on transport \Device\Nbf_Ibmtok51
```

stats [computer] This shows the browsing statistics of the computer.

getpdc transport domain This shows the NetBIOS name of the primary domain controller for the domain.

getmaster transp. domain This shows the master browser name for the domain.

getblist transport This lists master and backup browser servers.

listwfw domain This lists WFW servers that are running browser.

view transp. [srv | dom] This requests a browse list for selected transport. You can select the browse list from specific server (srv) or domain (dom). The flags that are used in this list can be seen by entering the browstat command without parameters. Here is an example of the output:

```
Remoting NetServerEnum to \\AUSRES15 on transport \device\netbt_ibmtok51 with flags
13 entries returned. 13 total. 10 milliseconds

\\AUSRES03          NT   04.00 (W,S,NT,SS,PBR,BBR)
\\AUSRES05          NT   04.00 (W,S,NT,SS,PBR,BBR,MBR)
\\AUSRES06          NT   04.00 (W,S,NT,SS,PBR,BBR)
\\AUSRES08          NT   04.00 (W,S,NT,SS,PBR,BBR)
\\AUSRES10          NT   04.00 (W,S,NT,SS,PBR)
\\AUSRES11          NT   04.00 (W,S,NT,SS,PBR)
\\ISHIIY            W95  04.00 (W,S,WFW,PBR,W95)
\\ITSONICE          NT   04.02 (W,S,PQ,XN,NT,SS)  ITSO-Austin Samba Server
\\ITSONT00          NT   04.00 (W,S,PDC,NT,BBR,MBR)   ITSO Austin NT PDC
\\ITSONT01          NT   04.00 (W,S,BDC,PQ,NT,BBR)    ITSO Austin NT BDC
\\LV3030C           NT   01.00 (W,S,PQ,XN,NT,SS)  Fast Connect Server
\\LV3030D           NT   04.02 (W,S,PQ,XN,NT,SS,PBR)  Samba2 Server
\\VIPER             NT   04.00 (W,S,NT,SS,PBR)    ITSO Austin CD-ROM Burner system
```

elect transport domain   This forces an election on the selected domain.
tickle   This forces a remote master to stop.

A.4 Troubleshooting utilities on AIX

This section describes AIX tools for troubleshooting SMB protocol. SMB is not a native protocol on AIX; so, special utilities are not available, but you can still get valuable information from standard TCP/IP tools.

A.4.1 TCP/IP configuration checking

You can check the TCP/IP configuration on SMB server with the following standard utilities: ifconfig, ping, arp, netstat, route, nslookup.

A.4.2 TCP/IP protocol troubleshooting

There is no special utility on AIX for analyzing SMB protocol, but you can use one of the standard utilities for analyzing TCP/IP.

A.4.2.1 iptrace

iptrace is a utility for recording Internet packets received from configured interfaces. You can provide a filter to capture only important network data. You can trace only data between local and remote host (not between two remote hosts). The iptrace utility runs as a daemon, and you must stop it with the `kill` command. The trace data is written to a file that can then be processed with the `ipreport` command. The syntax for the iptrace utility is as follows:

```
   iptrace [ flags ] LogFile
```

You can use the following flags:

`-i` *`interface`* This defines the specific network interface.

`-P` *`protocol`* This defines the network protocol (number or entry from /etc/protocols)

`-p` *`port`* This defines the port number (number or entry from /etc/services).

`-s` *`host`* This defines the source host name or host IP address.

`-d` *`host`* This defines the destination host name or host IP address.

`-b` This changes -s or -d to bidirectional mode.

`-a` This suppresses ARP packets.

`-e` This enables promiscuous mode on network adapters that support this function.

You can see part of the output obtained from capturing the NetBIOS protocol (only port netbios-ssn) with ipreport in the following screen:

```
$ iptrace -a -p netbios-ssn -s lv3030b -b trace.out
$ kill $(ps -fe | grep iptrace | grep -v grep | cut -c9-16)
$ ipreport trace.out

...
====( 220 bytes received on interface tr0 )==== 01:42:12.313466462
802.5 packet

802.5 MAC header:
access control field = 10, frame control field = 40
[ src = 00:06:29:b7:24:0c, dst = 00:04:ac:62:c9:80]
802.2 LLC header:
dsap aa, ssap aa, ctrl 3, proto 0:0:0, type 800 (IP)
IP header breakdown:
        < SRC =    9.3.187.213 >  (lv3030c.itsc.austin.ibm.com)
        < DST =     9.53.195.11 >  (ausres10.austin.ibm.com)
        ip_v=4, ip_hl=20, ip_tos=0, ip_len=198, ip_id=51908, ip_off=0DF
        ip_ttl=22, ip_sum=3265, ip_p = 6 (TCP)
TCP header breakdown:
        <source port=1932, destination port=139(netbios-ssn) >
        th_seq=216bef8, th_ack=3a349002
        th_off=5, flags<PUSH | ACK>
        th_win=5836, th_sum=d8ea, th_urp=0
00000000     0000009a ff534d42 72000000 00000000     |.....SMBr.......|
00000010     00000000 00000000 00000000 0000c11d     |................|
00000020     00000132 00770002 5043204e 4554574f     |...2.w..PC NETWO|
00000030     524b2050 524f4752 414d2031 2e300002     |RK PROGRAM 1.0..|
00000040     4d494352 4f534f46 54204e45 54574f52     |MICROSOFT NETWOR|
00000050     4b532033 2e300002 444f5320 4c4d312e     |KS 3.0..DOS LM1.|
00000060     32583030 32000244 4f53204c 414e4d41     |2X002..DOS LANMA|
00000070     4e322e31 00025769 6e646f77 7320666f     |N2.1..Windows fo|
00000080     7220576f 726b6772 6f757073 20332e31     |r Workgroups 3.1|
00000090     6100024e 54204c4d 20302e31 3200         |a..NT LM 0.12.  |

====( 141 bytes transmitted on interface tr0 )==== 01:42:12.318337099

...
```

A.4.2.2 tcpdump

The `tcpdump` command prints out the headers of packets on a network interface. You can define expressions to select packets that you want to see. The basic syntax of the `tcpdump` command is:

```
tcpdump { flags } expression
```

Important flags are:

-c count This exits after receiving count packets.

-f This prints the foreign Internet address numerically, not symbolically.

-i interface This defines the interface to listen to. If not defined, tcpdump will select one available interface.

-I This (uppercase i) specifies immediate packet capture mode without waiting for the buffer to fill up.

-N This omits printing domain part of the host name (e.g. lv3030c instead of lv3030c.itsc.austin.ibm.com).

-q This quiets output. Output lines contains less protocol information and are therefore shorter.

-t This omits printing a timestamp on each line.

-tt This prints an unformated timestamp on each line.

-v This prints more packet information (TTL and the type of service).

We must define expressions to filter incoming packets. When *expression* is true, the packet is accepted. *Expression* consists of one or more *primitives*. The following are the important primitives:

`[ src | dst ] host host` This is true if the source or destination is a host with a specified host name. You can limit selection to only source or destination host with src and dst qualifiers.

`[ src | dst ] net net` This is true if the source or destination is a network with a specified net number. You can limit the selection to only the source or destination network with src and dst qualifiers.

`[ src | dst ] port port` This is true if the source or destination is a port with a specified port number. You can limit the selection to only the source or destination port with src and dst qualifiers.

`ip broadcast` This is true if the packet is an IP broadcast packet.

`ip multicast` This is true if the packet is an IP multicast packet.

`ip, arp, rarp` This is true if the packet is of the selected protocol type (ip, arp, or rarp).

`tcp, udp, icmp` This is true if the packet is of the selected IP protocol type (tcp, udp, or icmp).

You can combine these primitives together with the operators and, or, not and parentheses (they must be escaped - ’\)’). The following are some examples of expressions.

To show all traffic to and from the lv3030c computer, use:

```
host lv3030c
```

To show traffic to and from a machine with a specified IP address, use:

```
ip host 9.3.187.21
```

To show traffic from lv3030c to ausres10, use:

```
srchost lv3030c and dst host ausres10
```

To show NetBIOS traffic involving host lv3030c, use:

```
\( port netbios-ns or port netbios-dgm or port netbios-ssn \) and host
lv3030c
```

Same as the previous example:

```
\( port 137 or port 138 or port 139 \) and host lv3030c
```

The important ports for diagnosing the SMB protocol are as follows:

`netbios-ns` (port 137) is the NetBIOS Name Service.

`netbios-dgm` (port 138) is the NetBIOS Datagram Service.

`netbios-ssn` (port 139) is the NetBIOS Session Service.

If you want to see, for example, the packet traffic between client and server, when the client runs the `net view` command, the client output will look like the following screen:

```
C:\>net view \\lv3030c
Shared resources at \\lv3030c

Samba Server

Share name   Type         Used as  Comment

-------------------------------------------------------------------------------
FINAL1       Print                 Lexmark Optra N
HOME         Disk                  User's Home Directory Share
TMP          Disk         X:
The command completed successfully.
```

On an AIX server, you can see the network traffic during this command as shown in the following screen:

```
$ tcpdump -t -N \(port 137 or port 138 or port 139\) and host lv3030c
LV3030B.1056 > lv3030c.netbios-ssn: P 841:945(104) ack 662 win 8099 (DF)
lv3030c.netbios-ssn > LV3030B.1056: P 662:701(39) ack 945 win 65535
lv3030c.netbios-ssn > LV3030B.1056: P 662:701(39) ack 945 win 65535
LV3030B.1056 > lv3030c.netbios-ssn: P 945:1060(115) ack 701 win 8060 (DF)
lv3030c.netbios-ssn > LV3030B.1056: P 701:992(291) ack 1060 win 65535
lv3030c.netbios-ssn > LV3030B.1056: P 701:992(291) ack 1060 win 65535
LV3030B.1056 > lv3030c.netbios-ssn: P 1060:1164(104) ack 992 win 7769 (DF)
lv3030c.netbios-ssn > LV3030B.1056: P 992:1031(39) ack 1164 win 65535
lv3030c.netbios-ssn > LV3030B.1056: P 992:1031(39) ack 1164 win 65535
LV3030B.1056 > lv3030c.netbios-ssn: P 1164:1279(115) ack 1031 win 7730 (DF)
lv3030c.netbios-ssn > LV3030B.1056: P 1031:1143(112) ack 1279 win 65535
lv3030c.netbios-ssn > LV3030B.1056: P 1031:1143(112) ack 1279 win 65535
LV3030B.1056 > lv3030c.netbios-ssn: . ack 1143 win 7618 (DF)
```

The `tcpdump` command does not support SMB protocol specifics. Extension to tcpdump source code is known under the name tcpdump-smb. At the time of this writing, no compiled version of this utility was available for the AIX system.

A.5 Common problems

Here is a list of some common problems and hints with the Samba server.

A.5.1 NetBIOS name resolution

Check the NetBIOS name resolution (WINS service):

- Use the `ping` command on the client with its NetBIOS name, its TCP/IP name, and its IP address to see whether the name translation works. If the ping to IP address works, but not with the NetBIOS name, you have a name resolution problem.
- Use the `ping` command with the WINS server IP address to see whether you can reach the WINS server.
- Double check the WINS server settings on the client and the status of your WINS server. You can check the WINS server settings on your client by selecting **Start -> Settings -> Control Panel -> Network -> Protocols -> TCP/IP Protocol -> Properties -> WINS Address**. To find the WINS server status on Windows NT, select **Start -> Settings -> Control Panel -> Services**, and then locate the Windows Internet Name Service. If the Status field is *Started*, WINS is running on the server.
- Enable LMHOSTS for name resolution and add an entry to the LMHOSTS file. You will enable LMHOSTS for name resolution by selecting **Start -> Settings -> Control Panel -> Network -> Protocols -> TCP/IP Protocol**

-> Properties -> WINS Address. Then, check the **Enable LMHOSTS Lookup** check box. If you want to resolve the host name of a machine, lv3030c, with IP address 9.3.187.213, you would add the following line into C:\winnt\system32\drivers\etc\LMHOSTS:

```
9.3.187.213 lv3030c
```

- Use the `nbtstat` command on the client for checking NetBIOS name resolution.

A.5.2 Browsing

Check the resource browsing on the client by using the following commands:

- Use `net view` to get the list of all visible computers on the network.
- Use `net view \\`*NetBIOS_name* to see the resources on single server.
- Use `browstat` for detailed information.

A.5.3 Authentication

Check whether the guest account is enabled and whether the guest user name is appropriate for an AIX user.

A.5.4 Netlogon

Sometimes, you may experience problems when working with the User profiles and System policies. You can use some tools and hints to deal with this.

Checking if the startup script runs

If you are not sure if the startup script runs, when a user logs in, add the `pause` command to the script. You should see a window at the login, waiting on your input.

Disable the local profile

If you are not sure, whether your local or remote profile is used, make the following registry change to use only remote profile (clear local profile on exit):

```
My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current
Version\WinLogon\DeleteRoamingCache=1 (DWORD)
```

Remove profiles

If you want to remove a complete profile for a user on a single computer, you can use the `delprof` command. It is located on a Windows NT Server

Resource Kit, version 4.0. The basic syntax for the `delprof` command is as follows:

```
delprof [/p] [/c:\\computer]
```

The flags are:

`/p`	Prompt before deleting profile
`/c:\\`*`computer`*	Specify remote computer

Enable logging of a user profile actions

You can use the checked version of the UserEnv.dll library, which is located on Windows NT Device Driver Kit (DDK) or Windows NT Software Development Kit (SDK). The steps to use this library are:

1. rename %systemroot%\system32\UserEnv.dll to UserEnv.old.
2. Copy the checked version of UserEnv.dll to %systemroot%\system32.
3. Start regedt32, and, in the path, enter:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\Winlogon
   ```

   Create the new value, UserEnvDebugLevel (REG_DWORD), with the value 10002.
4. Reboot the computer.

Logging information is recorded in the C:\UserEnv.log.

A.5.5 File system shares

- Check file and directory owner and access permissions on the server.
- Check the Samba umask setting on the server.

A.5.6 Printer share

- Check a direct printing from the AIX print queue on the server.
- Check and compare the printer definition on both server and client.
- Create a file on the the client (using the print to file option), transfer it to server, and try to print directly from there.

Appendix B. Special notices

This publication is intended to help AIX System Administrators to install and configure Samba on AIX, additionally it serves as a guide to server sizing and performance. The information in this publication is intended to act as an adjunct to existing Samba documentation and should not be read in isolation. See the RELATED PUBLICATIONS section 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, North Castle Drive, Armonk, NY 10504-1785.

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 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.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

IBM
OS/2
S/390
SP
Netfinity
RS/6000
SecureWay
System/390

The following terms are trademarks of other companies:

Tivoli, Manage. Anything. Anywhere.,The Power To Manage., Anything. Anywhere.,TME, NetView, Cross-Site, Tivoli Ready, Tivoli Certified, Planet Tivoli, and Tivoli Enterprise are trademarks or registered trademarks of Tivoli Systems Inc., an IBM company, in the United States, other countries, or both. In Denmark, Tivoli is a trademark licensed from Kjøbenhavns Sommer - Tivoli A/S.

C-bus is a trademark of Corollary, Inc. in the United States and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States and/or other countries.

PC Direct is a trademark of Ziff Communications Company in the United States and/or other countries and is used by IBM Corporation under license.

ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States and/or other countries.

UNIX is a registered trademark in the United States and other countries licensed exclusively through The Open Group.

SET and the SET logo are trademarks owned by SET Secure Electronic Transaction LLC.

Other company, product, and service names may be trademarks or service marks of others.

Appendix C. Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

C.1 IBM Redbooks

For information on ordering these publications see “How to get IBM Redbooks” on page 211.

- *AIX and Windows NT: Solutions for Interoperability*, SG24-5102
- *AIX Logical Volume Manager, from A to Z: Introduction and Concepts*, SG24-5432
- *S/390 File and Print Serving*, SG24-5330
- *Understanding IBM RS6000 Performance and Sizing*, SG24-4810

C.2 IBM Redbooks collections

Redbooks are also available on the following CD-ROMs. Click the CD-ROMs button at http://www.redbooks.ibm.com/ for information about all the CD-ROMs offered, updates and formats.

CD-ROM Title	**Collection Kit Number**
System/390 Redbooks Collection	SK2T-2177
IBM Networking Redbooks Collection	SK2T-6022
Transaction Processing and Data Management Redbooks Collection	SK2T-8038
Lotus Redbooks Collection	SK2T-8039
Tivoli Redbooks Collection	SK2T-8044
AS/400 Redbooks Collection	SK2T-2849
Netfinity Hardware and Software Redbooks Collection	SK2T-8046
RS/6000 Redbooks Collection (BkMgr)	SK2T-8040
RS/6000 Redbooks Collection (PDF Format)	SK2T-8043
Application Development Redbooks Collection	SK2T-8037
IBM Enterprise Storage and Systems Management Solutions	SK3T-3694

C.3 Other resources

This publication is also relevant as a further information source:

Using Samba, O’Rielly & Associates, ISBN 1-5659-2449-5

C.4 Referenced Web sites

These Web sites are also relevant as further information sources:

- `http://www.samba.org/`
  Samba project home page
- `http://www.ibm.com/rs6000/`
  IBM RS/6000 home page
- `http://www.kneschke.de/projekte/samba_tng/index.php3/`
  Samba TNG FAQ
- `http://www.cyclic.com`
- `ftp://ftp.gnu.org/gnu/rcs`
- `http://www-frec.bull.com/docs/download.htm`
- `http://us1.samba.org/samba/ftp/samba-latest.tar.gz`
- `http://us1.samba.org/samba/ftp/Binary_Packages/`
- `ftp://ftp.samba.org/pub/samba/samba-latest.tar.gz`
- `http://us1.samba.org/samba/docs/`
- `http://us1.samba.org/samba/support/`
- `http://web.mit.edu/pismere/directory-services/migration-4to5.html`
- `ftp://ftp.microsoft.com/Softlib/MSLFILES/NEXUS.EXE`
- `ftp://ftp.microsoft.com/Softlib/MSLFILES/SRVTOOLS.EXE`
- `http://www.microsoft.com/windows/zak/getzak.htm`
- `http://samba.org/cvs.html`
- `http://www.rs6000.ibm.com/doc_link/en_US/a_doc_lib/aixbman/admnconc/sys_res_overview.htm`
- `http://www-4.ibm.com/software/network/dispatcher/library`
- `http://www.rs6000.ibm.com/resource/technology/sp_papers/vsd.html`
- `http://www.rs6000.ibm.com/resource/aix_resource/sp_books/rvsd/index.html`
- `http://www.rs6000.ibm.com/resource/aix_resource/sp_books/gpfs/`
- `http://www.redbooks.ibm.com/portals/rs6000`
- `http://support.microsoft.com/support/tshoot/nt4_tcp.asp`

How to get IBM Redbooks

This section explains how both customers and IBM employees can find out about IBM Redbooks, redpieces, and CD-ROMs. A form for ordering books and CD-ROMs by fax or e-mail is also provided.

- **Redbooks Web Site ibm.com/redbooks**

  Search for, view, download, or order hardcopy/CD-ROM Redbooks from the Redbooks Web site. Also read redpieces and download additional materials (code samples or diskette/CD-ROM images) from this Redbooks site.

  Redpieces are Redbooks in progress; not all Redbooks become redpieces and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

- **E-mail Orders**

  Send orders by e-mail including information from the IBM Redbooks fax order form to:

	e-mail address
In United States or Canada	pubscan@us.ibm.com
Outside North America	Contact information is in the "How to Order" section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl

- **Telephone Orders**

United States (toll free)	1-800-879-2755
Canada (toll free)	1-800-IBM-4YOU
Outside North America	Country coordinator phone number is in the "How to Order" section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl

- **Fax Orders**

United States (toll free)	1-800-445-9269
Canada	1-403-267-4455
Outside North America	Fax phone number is in the "How to Order" section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl

This information was current at the time of publication, but is continually subject to change. The latest information may be found at the Redbooks Web site.

IBM Intranet for Employees

IBM employees may register for information on workshops, residencies, and Redbooks by accessing the IBM Intranet Web site at http://w3.itso.ibm.com/ and clicking the ITSO Mailing List button. Look in the Materials repository for workshops, presentations, papers, and Web pages developed and written by the ITSO technical professionals; click the Additional Materials button. Employees may access MyNews at http://w3.ibm.com/ for redbook, residency, and workshop announcements.

IBM Redbooks fax 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.

Abbreviations and acronyms

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
IBM	International Business Machines Corporation
iFOR/LS	Information for Operation Retrieval/License System
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	Network 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 UNIX Client
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

IBM Redbooks review

Your feedback is valued by the Redbook authors. In particular we are interested in situations where a Redbook "made the difference" in a task or problem you encountered. Using one of the following methods, **please review the Redbook, addressing value, subject matter, structure, depth and quality as appropriate.**

- Use the online **Contact us** review redbook form found at **ibm.com**/redbooks
- Fax this form to: USA International Access Code + 1 914 432 8264
- Send your comments in an Internet note to redbook@us.ibm.com

Document Number **Redbook Title**	SG24-6004-00 Samba Installation, Configuration, and Sizing Guide
Review	
What other subjects would you like to see IBM Redbooks address?	
Please rate your overall satisfaction:	O Very Good O Good O Average O Poor
Please identify yourself as belonging to one of the following groups:	O Customer O Business Partner O Solution Developer O IBM, Lotus or Tivoli Employee O None of the above
Your email address: The data you provide here may be used to provide you with information from IBM or our business partners about our products, services or activities.	 O Please do not use the information collected here for future marketing or promotional contacts or other communications beyond the scope of this transaction.
Questions about IBM's privacy policy?	The following link explains how we protect your personal information. **ibm.com**/privacy/yourprivacy/

IBM

Redbooks

Samba Installation, Configuration, and Sizing Guide

IBM®

Samba

Installation, Configuration, and Sizing Guide

Redbooks

Easy installation and customization of Samba on AIX

Advanced integration with HACMP and IBM Network Dispatcher

Practical sizing guidelines for CPU, memory, and network

Samba is the very popular open source software suite that lets you turn your AIX server into a file and print server for your PCs on the network. Samba is freely-available under the GNU General Public License.

There are many books that describe how to fully customize Samba. This redbook has a different approach: It gives you the basics of installing and configuring Samba on AIX using SWAT (the graphical interface) and discusses the different security models and how to configure PC clients, such as Windows 95, 98, NT, 2000, or OS/2. It also focuses on very specific AIX integration features, such as building a highly-available Samba server using IBM HACMP or a very scalable one using IBM Network Dispatcher. Last but not least, it provides sizing guidelines to help you select the most appropriate server for your environment.

If you have decided to go for Samba on AIX for your networking environment and you want to know more about how to exploit its powerful capabilities, this redbook is for you.

SG24-6004-00 ISBN 0738418528