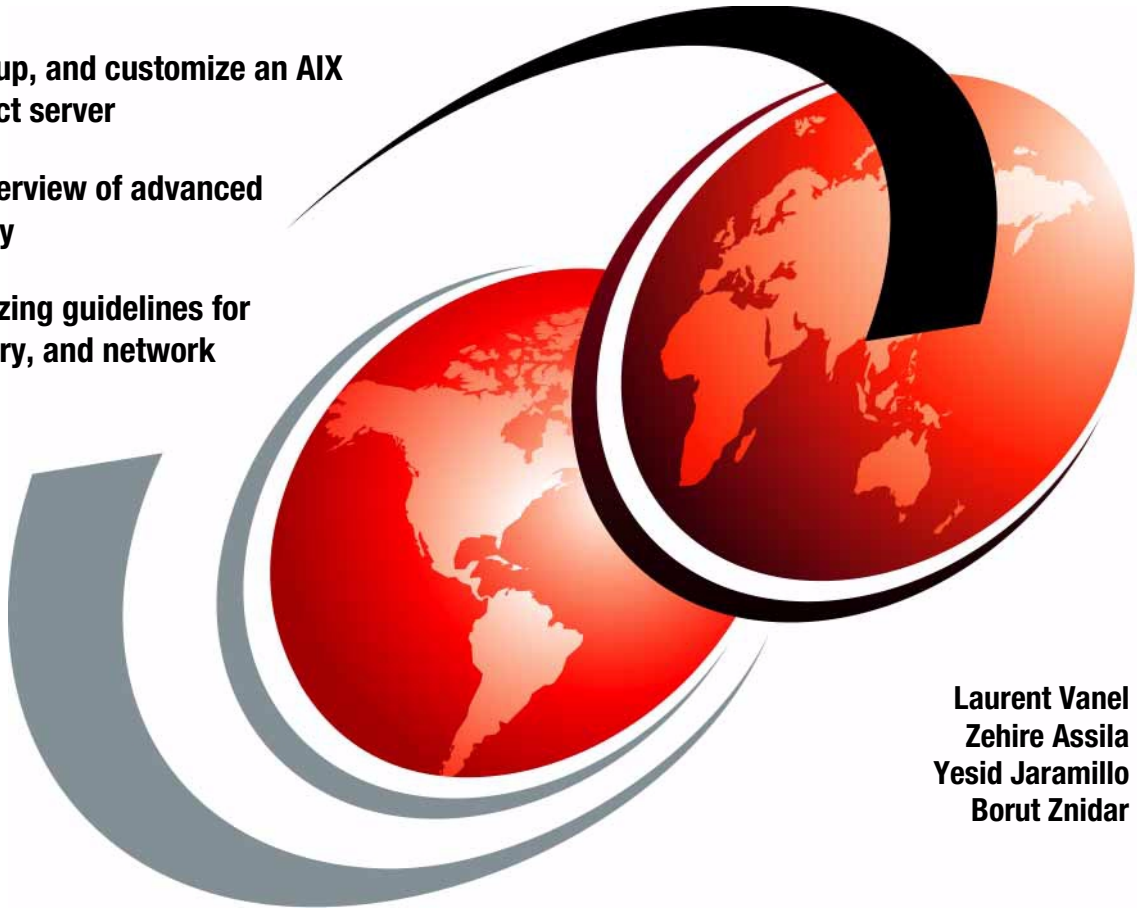
IBM

AIX Fast Connect
Functions and Sizing Guide

- Install, set up, and customize an AIX Fast Connect server
- Detailed overview of advanced functionality
- Practical sizing guidelines for CPU, memory, and network



Laurent Vanel
Zehire Assila
Yesid Jaramillo
Borut Znidar

ibm.com/redbooks

Redbooks

SG24-5527-00

International Technical Support Organization

AIX Fast Connect Functions and Sizing Guide

June 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 187.

First Edition (June 2000)

This edition applies to AIX Version 4.3, Program Number 5765-C34, and AIX Fast Connect for Windows and OS/2 Program Number 5765-C34-4101.

This document created or updated on June 23, 2000.

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

Preface

AIX Fast Connect allows PC file and print servers to be consolidated into a larger single AIX file and print server for enhanced manageability. As a part of AIX, the Fast Connect features can take advantage of existing and future core benefits including reliability, availability, scalability, open standards, security, systems management, performance, national language support, and IBM worldwide service and support.

This book explains how to install and set up an AIX Fast Connect server, how to declare file and printer shares, and how to choose the best security model that fits your needs.

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 AIX Fast Connect server.

Finally, you will find some sizing guidelines for Fast Connect and information on what server and configuration to choose based on the number of PC clients and the level of activity in your environment.

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 and RS/6000 specialist at the International Technical Support Organization, Austin Center. Before joining the ITSO three years ago, Laurent worked in the French RISC System/6000 Technical Center in Paris, where he conducted benchmarks and presentations for AIX and RS/6000 solutions.

Zehire Assila is an IT software specialist in France and has four years experience in the network support center in Paris (Marne-la-vallee). He has four years experience with SNA, X25, TCPIP, and NetBIOS in the AIX environment. Since then, he has provided AIX network support to both IBM IT specialists and customers.

Yesid Jaramillo has a bachelors degree in computer science. He is an IT specialist and works for Productora de Software S.A., an IBM Business partner in Colombia. He has more than six years experience working with IBM products, especially RS/6000 and AIX. He is certified in AIX 4.3

Administration and AIX 4.3 Support and is also a Microsoft Certified System Engineer.

Borut Znidar is an IT Specialist in IBM Slovenia and works in pre-sales support for AIX in ITC Ljubljana. Prior to that, he worked in Global services and AIX L2 support. He has worked for IBM since March 1998.

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

Ed Ponzini
AIX Architecture

Jay Ashford
AIX Architecture

Rakesh Sharma
IBM RISC System Division, Austin, Texas

Randall Preston
IBM RISC System Division, Austin, Texas

William Quinn
IBM RISC System Division, Austin, Texas

Joey James
IBM RISC System Division, Austin, Texas

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 201 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 Windows name resolution

The Windows name resolution process is the mechanism used to map the logical name you give a computer to its network address. The naming convention is based on the Network Basic Input/Output System (NetBIOS) protocol. Windows can use NetBIOS over several protocols, such as NetBEUI or TCP/IP. Since it is the protocol used by the AIX Fast Connect product, in this book, we will focus on NetBIOS over TCP/IP (the NetBT interface) as specified on RFCs 1001 and 1002.

The name resolution mechanism varies with the type of node (B, P,M, or H), and the configuration of the local system; so, it is necessary to present the network services that are potentially available.

Note

The NetBIOS name of one machine is unique and different from the DNS name, but it can be the same.

1.1 Name resolution mechanisms

There are different ways to resolve a NetBIOS name, and, depending on the type of node, the system will use these mechanisms or not. Here are the different mechanisms:

- NetBIOS cache
- NetBIOS name server
- IP subnet broadcast
- LmHosts file
- Hosts file
- DNS server

Early implementations only used cache information, IP subnet broadcast, and the Hosts and LmHosts files. The latest versions have modifications that add domain suffixes to the NetBIOS names in order to query the DNS. The maximum length of a NetBIOS name is fifteen characters, and the domain suffix is not considered part of the NetBIOS name.

1.1.1 The meaning of the 16th byte in NetBIOS names

We have just seen that the length for a NetBIOS name was fifteen characters. There is a hidden sixteenth byte used to identify the type of node and the role

performed by this node. The possible meanings of this sixteenth byte are divided into two groups:

Computer names:

\00	All registered machines have a unique record of this type; this is the name referred in the NetBIOS computer.
\03	Registered on a WINS server-like messenger service on a computer that is a WINS client.
\06	Used to specify Remote Access Server (RAS) service.
\1B	Used for the domain master browser. Only the PDC (Primary Domain Controller) can have this record type.
\1F	Used to specify Network Dynamic Data Exchange (NetDDE).
\20	Used to specify server names and provide shared resources, such as files or printers.
\21	Used to specify RAS clients.
\BE	Used to specify that the network monitor agent is used on the computer.
\BF	Used to specify that the network monitor utility is used on the computer.

Group names:

\1C	Used to specify a domain group name.
\1D	Used to specify the master browser.
\1E	Used to specify normal group names.
\20	Used to specify special group names.
MSBROWSE	Used to periodically announce their domain records of the local subnet by master browser servers.

1.2 Types of nodes

The NetBIOS definition on RFCs 1001 and 1002 specifies different nodes. All these types are supported in a Windows environment, even if some of them are not generally used.

1.2.1 B node

The B node uses broadcast messages for the registration and resolution of the names. This type of node may not be adequate in large networks since it significantly increases network traffic.

1.2.2 P node

The P node sends broadcast messages to NetBIOS name servers, such as WINS servers, for name registration and resolution. This type of node avoids the network load because the broadcast messages are only sent between the server and the node client (point-to-point) for the registration and resolution process. If there is not an active NetBIOS name server on the network, name resolution fails.

1.2.3 M node

The M node is a mix of B and P nodes. The computer first attempts registration and resolution acting as a B node; if this fails, it acts as a P node. The advantage of this type of node is that it can be used across routers and, in theory, should improve network performance.

1.2.4 H node

The H node solves problems associated with broadcasts and routed environments. It is also a combination of B and P nodes and can be configured to use the LmHOSTS file.

This type of computer first acts as a P node for name registration and resolution, then as a B node if the first step has failed. If none of the Windows native name resolution methods was successful, the machine will check the LmHOSTS file; then, if the DNS server is defined, it will send a query to the DNS server.

If everything fails, the NetBIOS name stays unresolved.

1.2.5 How to change the node type

The type of node can be changed by modifying the registry database using the REGEDIT or REGEDT32 tools, which are provided with every version of the Windows products.

All Microsoft Windows operating systems use the B-node as a default, but, if the machine has been configured to use a WINS or NetBIOS Name Server (NBNS), H-node becomes the default node type.

1.2.5.1 Changing the node type on Windows NT

To change the node type on machines with Windows NT installed, it is necessary to modify or create *the NodeType* value with the *Reg_DWord* type in the following *Key:*

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netbt\Parameters
```

The valid values can be 1, 2, 4, 8 (B node, P node, M node, H node).

1.2.5.2 Changing the node type on Windows 9X

To change the node type on machines with Windows NT installed, it is necessary to modify or create *the NodeType* value with the *Reg_DWord* type in the following *Key:*

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\VxD\MSTCP
```

The valid values can be 1, 2, 4, 8 (**B node**, P node, M node, **H node**).

Note

It is not necessary to manually change the type of node. This is done automatically when you configure a new protocol or define a WINS or DNS Server, HOSTS, and LmHOSTS files; however, if necessary, it can be changed.

1.3 Machine roles in the browsing mechanism

A machine installed with any product of the Windows family can participate in the Windows name resolution and browsing mechanism. The five types of roles possible for a system are described in the following short sections.

1.3.1 Non-browser

This is a computer with this role only does queries to the domain master browser, master browsers, or backup browsers. This role could be useful on laptop computers.

1.3.2 Potential browser

This is a network computer capable of keeping a list of the network resources (called a browse list) and can be elected master browser. A machine with this role can also be a backup browser if it is selected by the master browser.

1.3.3 Backup browser

The Backup Browser is any network computer running Windows NT server, Windows NT Workstation, Windows 9X, or Windows for Workgroups; The Domain Master Browser sends a copy of the resource browse list to the backup browsers every 15 minutes or when the backup browser requests it. Any machine running Windows NT Workstation, Windows 9X, or Windows for Workgroups can be selected to be the backup browser if there are less than three Windows NT servers acting as backup browsers.

1.3.4 Master browser

The master browser machine keeps a list of all the network resources on one segment of the network, resolves requests from the clients, and sends a copy of this list to the Domain Master Browser.

1.3.5 Domain master browser

This machine is always the Primary Domain Controller (PDC) of the domain. It is responsible for collecting information from the master browsers in each of the subnets included in its domain.

1.4 Definitions

In the following sections, we provide brief definitions of some components of the name resolution process.

1.4.1 What is the LmHOSTS file?

The LMHOSTS file is used to keep a list of NetBIOS names and their IP addresses. This file was the central point of information but was replaced by a NetBIOS Name Server, such as WINS server from Microsoft, to simplify the administration of large networks.

1.4.2 What is the Host file?

The HOSTS file is used to keep a list of machines names and their IP addresses. This file is still used, but, in some configurations, it is replaced by Domain Name Servers (DNS), such as the DNS server from Microsoft. Remember, the same machine can have a TCP/IP name different than its NetBIOS name. The Hosts file tracks the TCP/IP name where the LmHOSTS file tracks the NetBIOS name.

1.4.3 What is the WINS server?

The WINS server is a service that helps resolve NetBIOS names and maintains a distributed data base with IP addresses and NetBIOS names. it is based on RFCs (1001 and 1002). This service uses a dynamic database and prevents broadcast messages that can heavily load the network. It also provides an advantage in the ease of administration. This service supersedes the use of the LMHOSTS file.

1.4.4 What is the DNS?

The Domain Name Server (DNS) service is used to map HOST names to IP addresses; this service is widely used on the Internet and replaces the use of the HOSTS file.

1.5 Example of a NetBIOS name resolution process

We are going to show what happens on the computer when you use the Find a Computer application. See Figure 1.

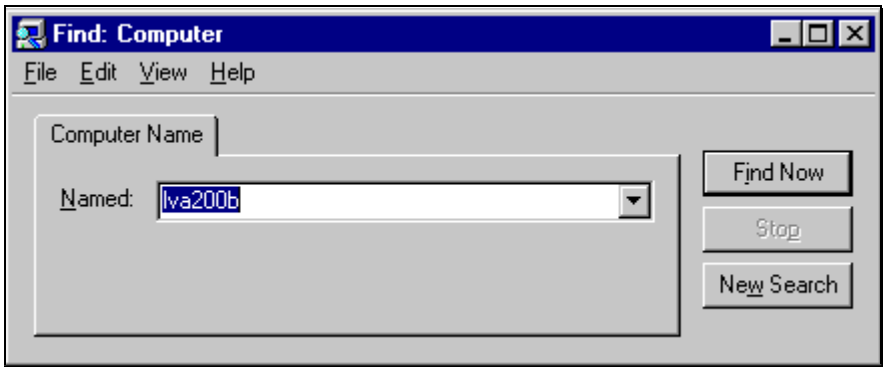


Figure 1. Finding a computer NetBIOS name with the Find Computer option

You have entered lva200b as the NetBIOS name to locate. The process used to resolve this name depends on the node type. The following steps are the sequence to resolve the name:

1. Check if the name has more than fifteen characters; if that is the case, we will first try to resolve the name with the DNS server
2. If it fails, the NetBIOS resolution fails; go to Step 5.
3. Check the type of node. If the node type is H, go to step 3; otherwise, go to step 4.

4. The node type is H. It checks the NetBIOS cache, checks the WINS server, uses broadcast, checks LmHOSTS file, checks the HOSTS file, and then uses the DNS. At every step, a positive answer is a success. Otherwise, the name resolution fails. Go to Step 5.
5. The node type is B. It uses the local cache information and a local broadcast. If none of these methods succeed, the name resolution fails. Go to Step 5.
6. End the name resolution process.

Chapter 2. Fast Connect presentation and installation

AIX Fast Connect for Windows and AIX Fast Connect for OS/2 are IBM products using the Microsoft networking protocol. PC clients can access AIX files and printers using their native networking client software.

We will use an RS/6000 running AIX Version 4.3.3 as the base platform for AIX Fast Connect for Windows 2.1.1.

2.1 AIX Fast Connect for Windows overview

AIX Fast Connect enables Windows and OS/2 clients to access AIX file systems and printers as if they were locally stored. AIX Fast Connect provides these services by implementing the Server Message Block (SMB) networking protocol. SMB uses Network Basic Input/Output System (NetBIOS) over the Transmission Control Protocol/Internet Protocol (TCP/IP).

Important features of Fast Connect include:

- Tight integration with AIX and use of features, such as threads, kernel I/O, file systems, and security.
- SMB-based file and print services. It is the protocol used by NetBIOS to implement Windows file sharing and print services.
- Client authentication can be done by Fast Connect server or through passthrough authentication to NT domains.
- Support for resource browsing protocol, such as Network Neighborhood and NET VIEW. The server can announce its resources on the network but it cannot be a master browser.
- Supports WINS client and proxy for B-node client and implements NetBIOS Name Server (NBNS).
- It can be managed by the *net* command, the Web-based System Manager, or the System Management Interface Tool (SMIT).
- Traces and logs capabilities.
- Support of unicode.
- AIX long file name to DOS file mapping support. This feature is needed for many older (16 bit) applications running under Windows 95, Windows 98, and Windows NT.

- For more information, see the AIX Version 4.3 Base documentation on Fast Connect in Chapter 11 of the book, *System Management guide: Communication and Networks*, SG23-2487.

  AIX Fast Connect is a licensed product. There is a unique price for the server, and there is no limit on the number of clients.

  An evaluation version of the AIX Fast Connect product is included in the Bonus Pack for AIX Version 4.3, announced June 8, 1999.

2.2 AIX Fast Connect for Windows requirements

This section describes hardware and software requirements, both for the AIX server and for its PC clients.

2.2.1 Server hardware requirements

AIX Fast Connect for Windows runs on any machine that supports AIX (except diskless and dataless machines). The machine must have a network adapter supporting the TCPIP protocol. The system must have at least 32 MB of RAM (64 MB is recommended) and 50 MB of available disk space.

2.2.2 Server software requirements

The server software requirements for Fast Connect are:

- AIX Version 4.3.2 or higher
- Fileset, bos.net.tcp.client 4.3.2.0 or higher, must be installed.
- Fileset, bos.rte.loc 4.3.2.2 or higher, must be installed.
- For AIX 4.3.2, APAR IX85388 is required for sendfile API support.

2.2.3 Client hardware requirements

Each pc must have a network adapter installed and physically connected to the network.

2.2.4 Client software requirements

The supported operating systems are:

- Windows NT 4.0
- Windows 98
- Windows 95 with service pack 1 or higher
- Windows for Workgroups 3.11 or higher

- OS/2 warp 4.0 or higher
- Windows 2000

To manage Fast Connect remotely with the Web-based System Manager tool, a Web browser is needed on the client with Java 1.1.2 support (for example, netscape 3.0 or higher).

2.3 Installation

This section describes Web-based System Manager (WebSM) installation and configuration as well as the AIX Fast Connect installation.

We can manage Fast Connect from WSM, the `net` command, or SMIT. In this book, we will use the Web-based System Manager interface. We will also provide the SMIT fast path and the related `net` command.

2.3.1 Installation of Web-based System Manager (WebSM)

To configure WebSM, perform the following steps:

1. Install the Web server.

We installed IBM HTTP Web Server 1.3.6.1. Other products are supported as well, but we need to know the path of the document directory. For the configuration of the IBM HTTP Web server, see the readme file in /usr/HTTPServer/readme directory.

To see if there is a Web server running, use the following command:

```
ps -ef |grep httpd
```

This should return the /usr/HTTPServer/bin/httpd process.

2. Test the Web server.

Start a browser (Netscape for example) and go to the URL, `http://hostname`. You should see the main page of your Web server software. If you get a problem, see the readme file for the configuration of your Web server.

3. Install WebSM.

to install WebSM, we have to install following filesets:

- sysmgt.help.en_US.websm
- sysmgt.help.msg.en_US.websm
- sysmgt.msg.en_US.websm.apps

- sysmgt.websm.apps
- sysmgt.websm.diag
- sysmgt.websm.framework
- sysmgt.websm.icons
- sysmgt.websm.rte
- sysmgt.websm.ucf
- sysmgt.websm.widgets

4. Find the document directory for websm.

You need to know the document directory for your Web server. For IBM HTTP server 1.3.6.1, the default path is /usr/HTTPServer/htdocs/en_US.

When the Web server is verified as installed and accessible, run the following command:

```
/usr/websm/bin/wsmappletcfg -docdir "your webserver docdir"
```

For example, for IBM HTTP server, this would be:

```
/usr/websm/bin/wsmappletcfg -docdir /usr/HTTPServer/htdocs/en_US
```

5. Enable the WebSM server by running the following command:

```
/usr/websm/bin/wsmserver -enable
```

Now, WebSM is configured on the system. You will need a compatible browser that supports Java 1.1, AWT 1.1-enabled Web browser. For more information, see /usr/websm/README file.

6. To access WebSM from a browser, enter the following:

```
Use the URL: http://yourservername/wsm.html
```

2.3.2 Installation of AIX Fast Connect

To install AIX Fast Connect, we have to install the following packages:

- *cifs.base* (Fast Connect server utilities: Commands, SMIT supports, and Web-Based System manager).
- *cifs.msg* (Fast Connect server messages: Language is indicated by the fileset extension).
- *cifs.basic* (Fast Connect server Files, it is for windows only)

or

- *cifs.advanced* (Fast Connect server files for windows and OS/2)

After the installation completes, on your WebSM client, open the following URL:

`http://server/wsm.html`

As shown in Figure 2, you will see an additional PC Services icon for Fast Connect on the main window of WebSM.

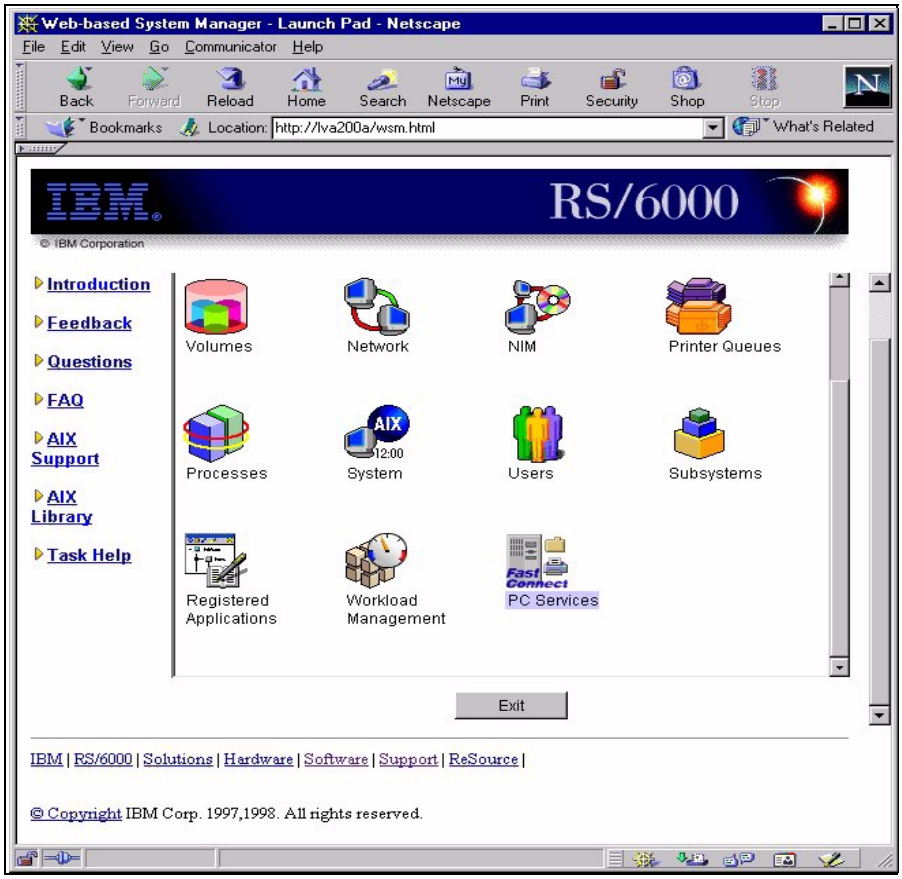


Figure 2. WebSM window

You can check the correct installation of the filesets by entering the following command: `lslpp -h "*cifs*"`

The output of this command is shown in the following screen:

```
cifs.base.cmd
                  2.1.1.0   COMMIT      COMPLETE    01/28/00    14:14:08
                  2.1.1.1   APPLY       COMPLETE    01/31/00    18:07:40
cifs.base.smit
                  2.1.1.0   COMMIT      COMPLETE    01/28/00    14:14:07
cifs.base.websm
                  2.1.1.0   COMMIT      COMPLETE    01/28/00    14:14:07
cifs.basic.rte
                  2.1.1.0   COMMIT      COMPLETE    01/28/00    14:14:39
                  2.1.1.2   APPLY       COMPLETE    01/31/00    18:07:49
cifs.msg.en_US
                  2.1.1.0   COMMIT      COMPLETE    01/28/00    14:14:30
```

Note

You must install cifs.basic or cifs.advanced packages but not both at the same time, or the installation process will fail.

Chapter 3. Defining shares

You can configure AIX Fast Connect with the Web-based System Manager (WebSM) or the `smit` or `net` commands.You can set the server properties and define file system shares or printer shares.

Only the root user is allowed to modify the configuration, but any user can access the configuration menu.

The modification of the most configured parameters (those called dynamic) does not require the server to be stopped and restarted for the changes to become effective.

3.1 Quick start

After the installation of the AIX Fast Connect product, you can start the server without any additional configuration.

When the server is started, a file share, named HOME, is created and loaded by default.

3.1.1 Starting/stopping the Fast Connect server

First, you can start the Fast Connect server from the *PC Services* icon in the WebSM main window.

When you start the server, you have three predefined file system shares: HOME, IBMLAN$, and ADMIN$. The last two are used by the server and cannot be accessed by clients.

The default server name is the AIX TCP/IP hostname, and the domain name is *WORKGROUP*.

You have three methods of starting the server:

1. From WebSM (see Figure 3 on page 16)
   a. Select the server line.
   b. Select **Selected / Start Server Operations**.
   c. Select one of the startup options: **immediately**, **on restart** or **both**.
2. From `smit`:
   a. smitty smb
   b. Select the **Start Server** option.

3. At the command line, enter the following:
   `net start /load`

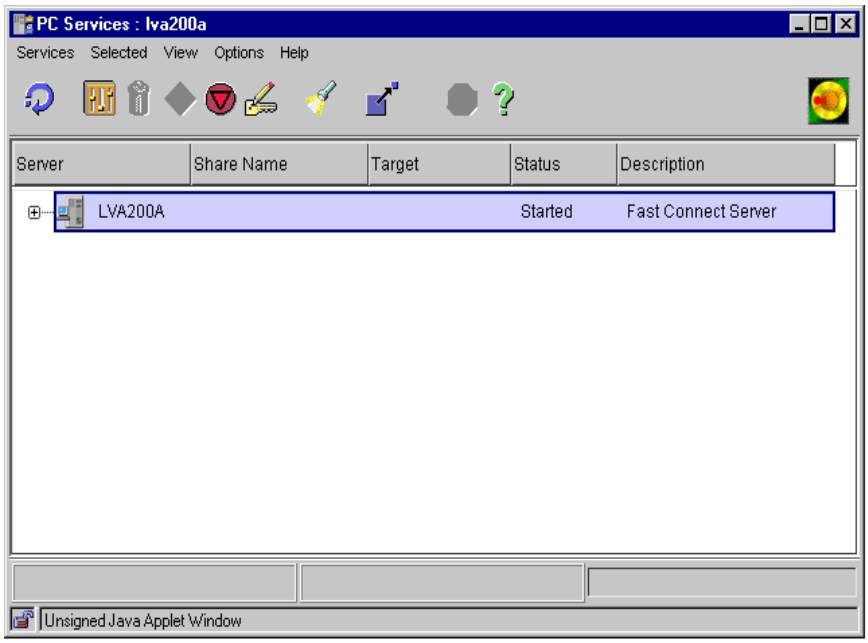


Figure 3. PC Services

To stop the server, you have the three methods just described:

1. From WebSM:
   a. Select the server line.
   b. Select the **Selected / Stop Server Operations** option.
2. From SMIT:
   a. Enter `smitty smb`
   b. Select **Stop Server**
3. From the command line:

- Enter `net stop`

From WebSM, you can see that the server is running when the Status label is *Started*. From the command line, you can use `net status` command to check the status of the server.

3.1.2 Additional configuration

In this section, we will look at additional parameters that can be modified to make the server operational.

3.1.2.1 How to modify the domain name

The domain name is set to WORKGROUP by default. This is the domain to which this server belongs. The domain name is the name assigned to a group of servers that interoperate to provide resources. This name is used to locate your server in the Network Neighborhood program from client machines.

You can change the server domain by selecting **Selected/properties** from the WebSM menu of AIX Fast Connect server (see Figure 4 on page 18).

You can use SMIT fast path, `smitty smbcfghatt`.

At the command line, type: `net config /domainname:<d_name> (the name of the domain)`

3.1.2.2 How to modify the AIX Fast Connect name

The name of the Fast Connect server defaults to the TCP/IP hostname of the AIX machine. The server name is the NetBIOS name of the server. This name will be used by the clients to access the server. You can modify the server name in the Server Properties window (see Figure 4 on page 18).

You can use the smit fast path: `smitty smbcfghatt`

At the command line, type: `net config /servername:<s_name> (the name of the server)`

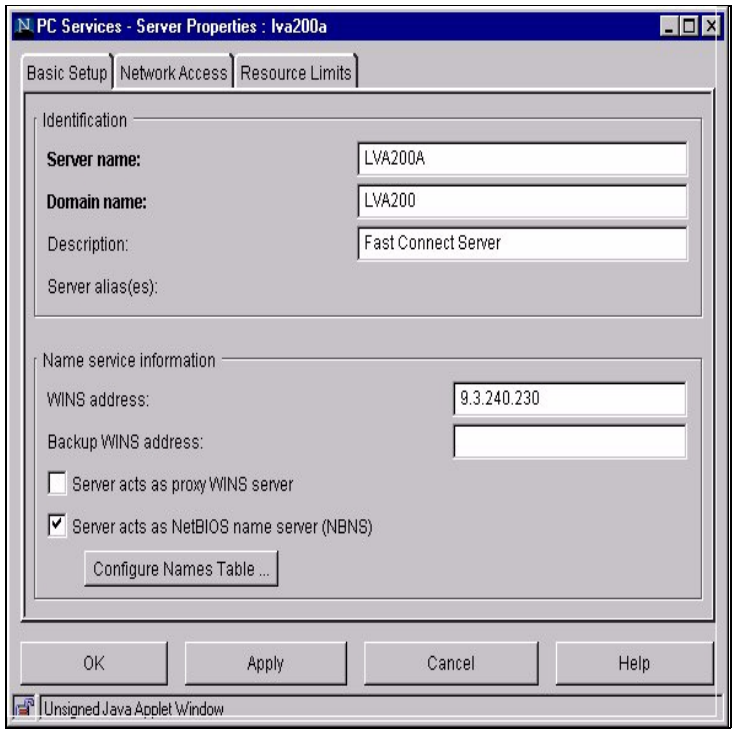


Figure 4. AIX Fast Connect server properties

3.1.2.3 Switching user

To modify the configuration of the Fast Connect server, you must be logged as root. From the WebSM menu of AIX Fast Connect, you can use `the switch user` function from the Services option to change the user login (see Figure 5 on page 19).

Select the **Services / Switch User** option.

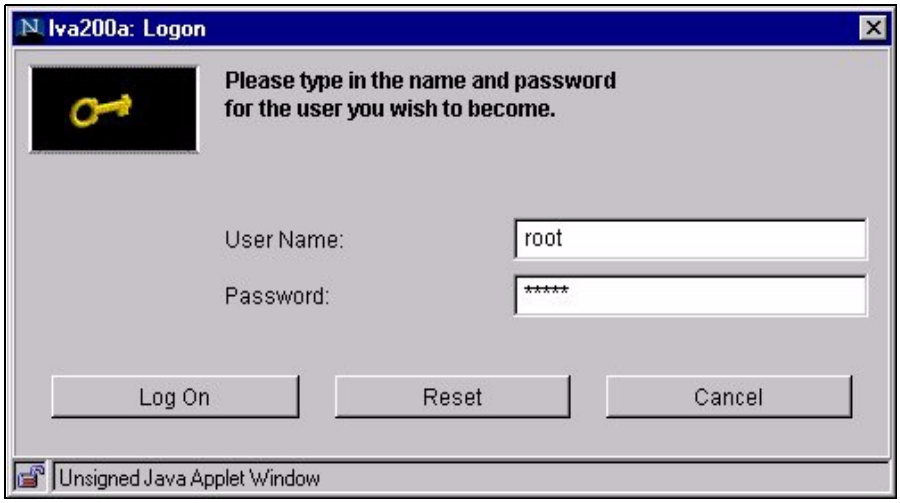


Figure 5. WebSM Logon panel

3.2 Defining file system shares

The server is now started with the correct attributes. It is now time to define new shares, files shares, and print shares. Let us start with file shares.

3.2.1 Adding or changing file system shares

Perform the following steps to add a new file system share:

1. Select **Services / New File system Share** from the WebSM menu (see Figure 6 on page 20) or select a shared file system and then select **Selected / Properties** from the WebSM menu if you want to change the properties of the share.
2. Enter the file system share name (for example, enter `TEST`). This is the logical name for the shared file system resource.
3. Enter the full absolute path for the shared file system (for example, enter `/home/pc/test`).
4. You can enter a brief description for this shared file system (for example, enter `test share`).
5. Click on **OK**.

All changes made to the file system share are immediately available.

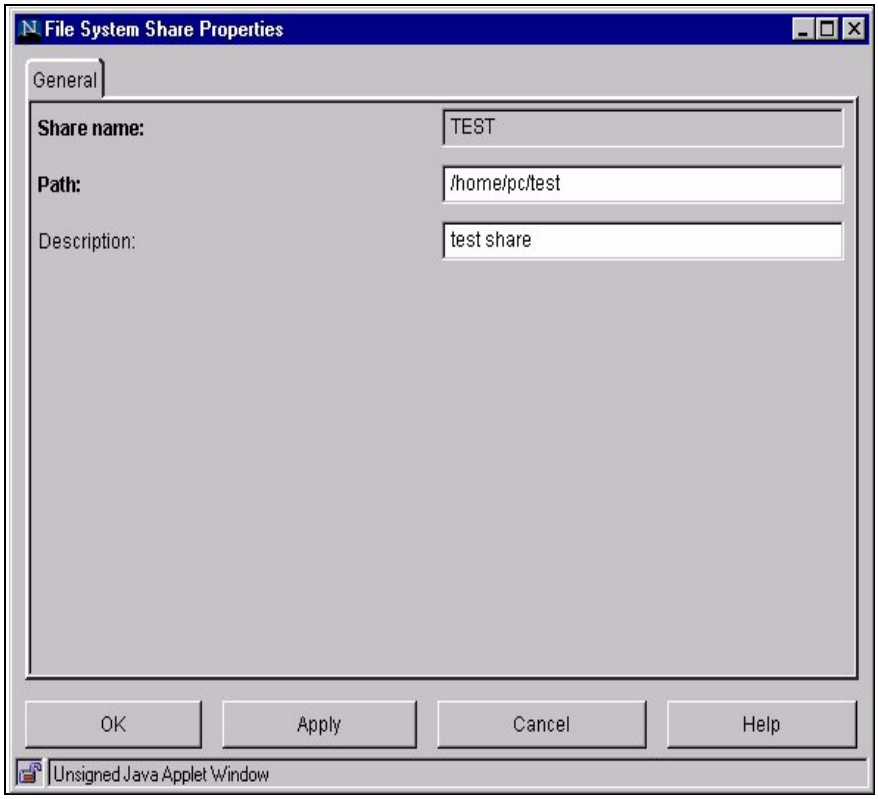


Figure 6. Defining file system share

You can use the following SMIT fast path:
`smitty smbsrvfiladd, smbsrvfilchg`

At the command line, enter: `net share /add /type:file /netname:<share_name> /path:<path_name>`

3.2.2 Deleting a file system share

If you want to delete a file system share from your server, first, select the share, and then select **Selected / Remove Share** from the WebSM menu.

You can use the following SMIT fast path:
`smitty smbsrvfilrm`

You can enter the following at the command line:
`net share /delete /netname:<share_name>`

3.3 Defining printer share

Defining printer shares is also easy, as described in the following section.

3.3.1 Defining printer on AIX

We use the Web-based System Manager to define shares that will be mapped to the printers on an AIX server. Perform the following steps:

1. Select the Printer Queues icon from the Web-Based System Manager window (see Figure 7 on page 22).
2. Select **Printer / new Queue and Printer** from the Printer Queues window (use the TaskGuide Method).
3. Type the queue name.
4. Choose the name of the AIX print queue (for example, we used remote).
5. Enter `remote server name` and `name of queue on remote server`.
6. Click **NEXT**.
7. If successful, you will get the following message:

   ```
   The following queue and destination have been successfully created.

   Queue name: 3130PS
   server name: itsont01
   ```

8. Click **Finish**.

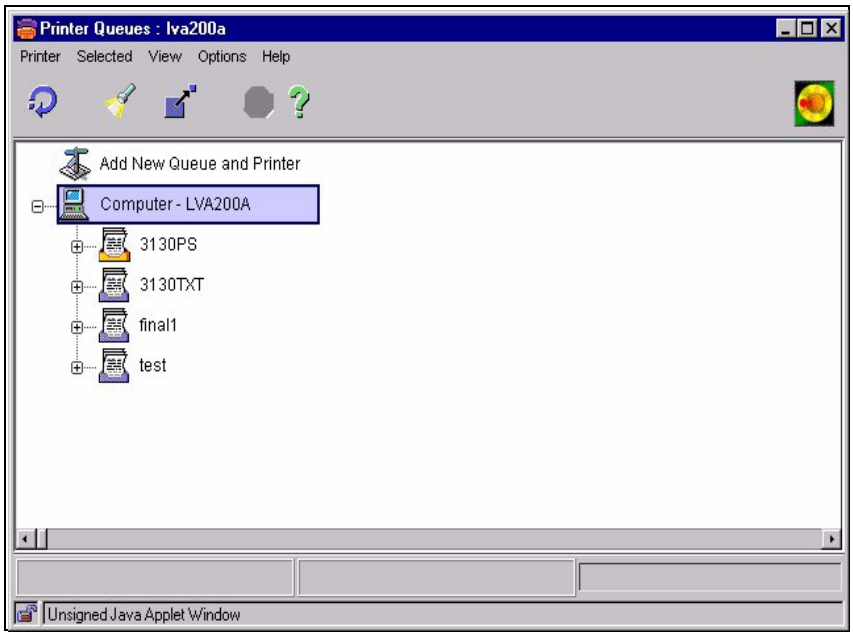


Figure 7. Defining a printer queue

3.3.2 Adding or changing printer share

Perform the following steps to create a printer share on your server:

1. To create a new printer share, select **Services / New printer Share...** from the WebSM menu, (see Figure 8 on page 23).

   If you want to modify the properties of a printer queue, select a shared printer queue in the window and select **Selected / Properties** from the WebSM menu.

2. Enter the printer share name (for example, enter: `3130PS`).
3. Enter an AIX printer queue name (for example, enter:`3130PS`). This queue can be associated with either a local or remote AIX printer.
4. You can, optionally, enter the description of this share (for example, enter: `IBM 3130 laserPrinter PS`). The description can help the client's users with printer installation if you specify the printer type in the description field.
5. You can, optionally, enter some printer options. This is a string field of options passed unmodified to the AIX `enq` command. This will allow you to provide special treatment to jobs coming from the clients.
6. Click on **OK**.

Any modifications made to the printer share configuration are immediately available.

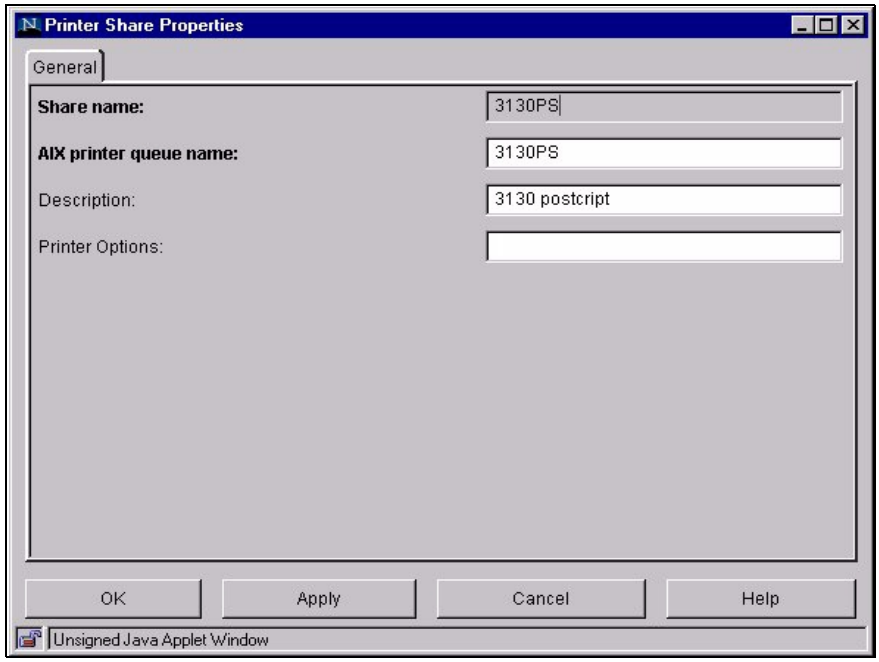


Figure 8. Defining printer share

You can use the following SMIT fast path:

```
smit smbsrvprtadd, smbsrvprtchg
```

Enter the following at the command line:

```
net share /add /type:printer /printq:<qname>
```

3.3.3 Deleting printer share

If you want to delete a printer share from your server, select the printer share and then select **Selected / Remove share** from the WebSM menu**.**

You can use the following SMIT fast path:

```
smit smbsrvprtrm
```

Type the following at the command line:

```
net share /delete /netname:<q_name>
```

Chapter 4. Accessing Fast Connect from Windows 95/98

Now that we have seen how to configure and start the Fast Connect server, we can start the client configuration. In this chapter, we will cover how to configure Windows 95 and Windows 98 clients (referred to as Windows 9x in this chapter) to access the server.

4.1 Windows configuration

You will see that it is very easy to configure the windows workstations. SMB is Microsoft Windows native language for resource sharing on a local area network. It uses TCP/IP to communicate with its clients on the network.

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. Perform the following steps to customize customize Windows 9x:

1. Click **Start -> Settings -> Control Panel** and double-click the **Passwords** icon. You will see the Passwords Properties dialog box shown in Figure 9 on page 26.

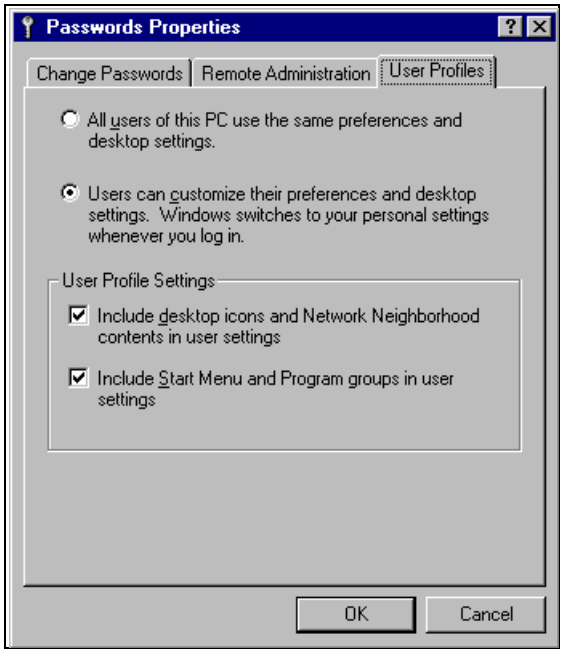


Figure 9. User Profiles

2. Select the **User profiles** tab, then click the lower of the two radio buttons. Now, click the **Change Passwords** tab. You should see the tab as shown in Figure 10 on page 27.

Figure 10. Change Windows passwords

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

3. Return to the Control Panel and select the **Network** icon. You should now see the Network dialog box shown in Figure 11 on page 28.

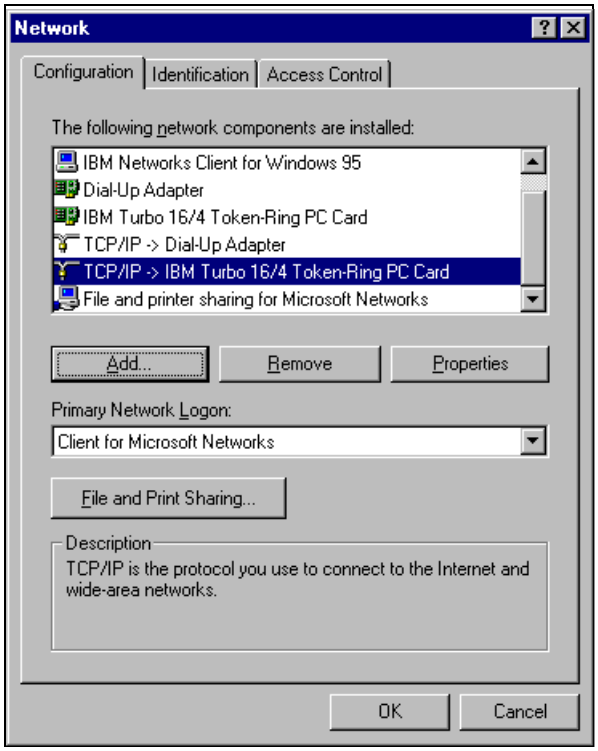


Figure 11. Network dialog box

4. Choose the TCP/IP protocol with the adapter with which you want to access the Fast Connect server, and click **Properties**. Select the **WINS Configuration** tab, and you should now see the dialog box shown in Figure 12 on page 29.

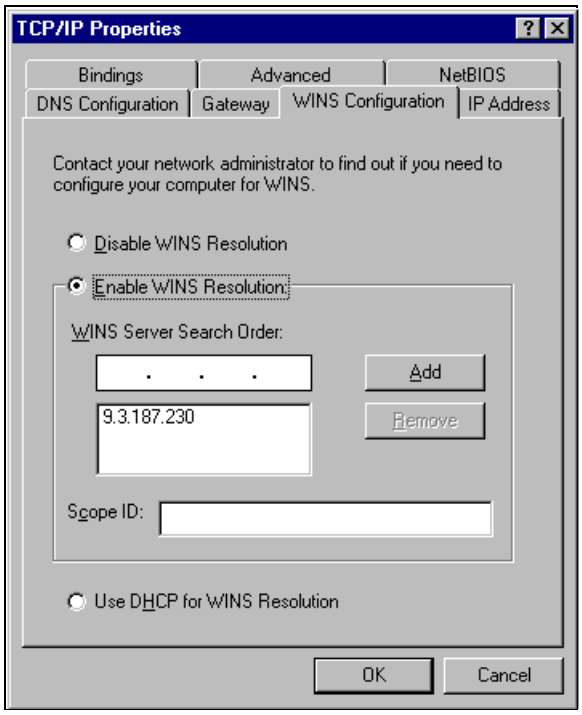


Figure 12. WINS Configuration

5. 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 the one in Figure 13 on page 30.

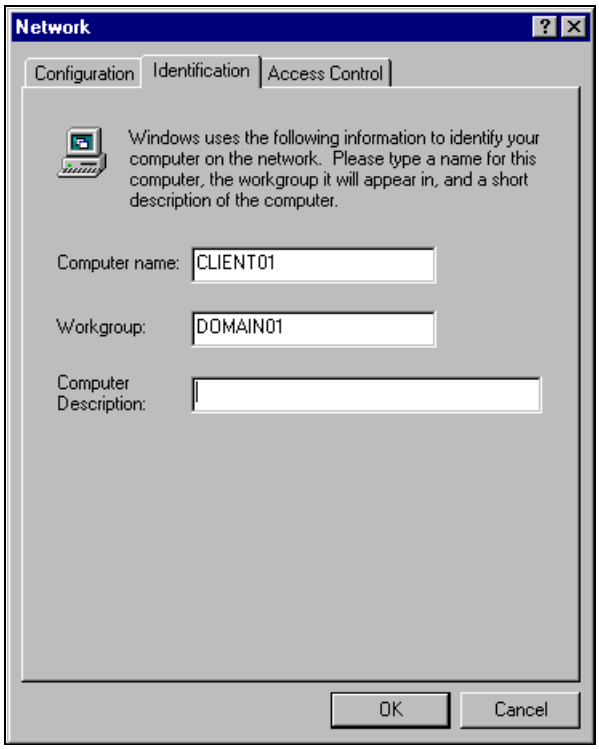


Figure 13. Windows 95/98 Identification

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

4.2 Accessing the Fast Connect server

You must have a valid Windows logon to get access from the AIX Fast Connect server. See Figure 14 on page 31 for an illustration of how to select the primary network logon to be a validated logon session.

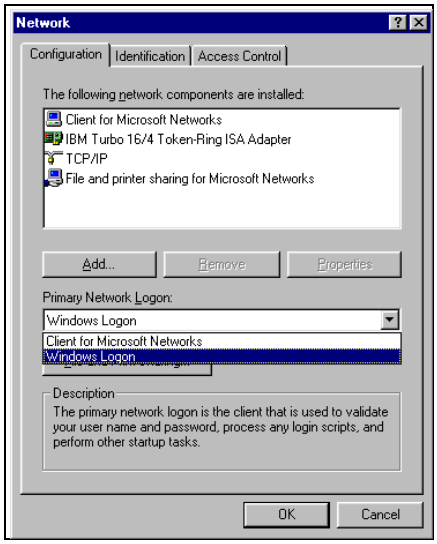


Figure 14. Select Primary Network logon

4.3 Locating the AIX Fast Connect server from Windows 9x

There are many ways to access an AIX Fast Connect server from standard Windows 9x clients. Here, 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
- AIX Fast Connect server: lva200a, lva200b
- NetBIOS name server (NBNS): lva200a

4.3.1 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 AIX Fast Connect 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 15.

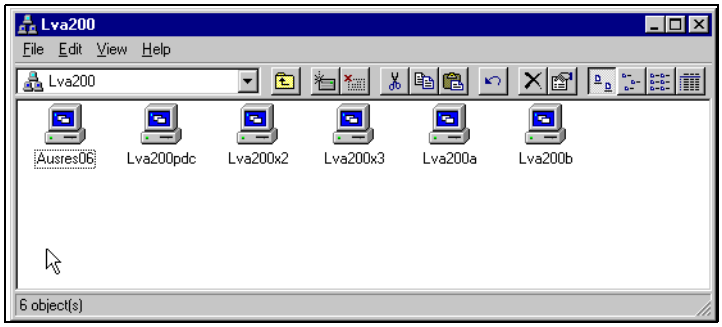


Figure 15. LVA200 domain

4.3.2 Using the Find Computer option

Another way to locate the AIX Fast Connect server is by using the Find Computer option. To find the AIX Fast Connect server (lva200b) using this option, perform the following this 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 AIX Fast Connect server to be located as shown in Figure 16 on page 33.

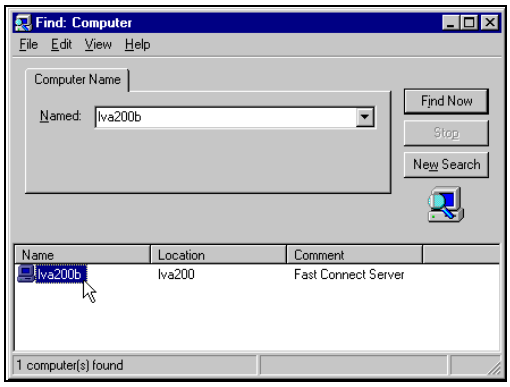


Figure 16. Find Computer

3. Select the **Find Now** option, and the AIX Fast Connect server will appear.

4.3.3 Using the command line

To locate the AIX Fast Connect 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 AIX Fast Connect server (lva200a) using this option, perform the following steps:

1. Open an MS-DOS command line interface by selecting the following: **Start -> Programs -> Command Prompt.**
2. Enter the following command to locate the AIX Fast Connect 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

Fast Connect 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 Fast Connect
\\LVA200B              Fast Connect 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.

4.4 Accessing resources from AIX Fast Connect server

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

4.4.1 Accessing files

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

4.4.1.1 GUI interface

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

Using a UNC name

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

1. After having located the AIX Fast Connect server (see Section 4.3, “Locating the AIX Fast Connect server from Windows 9x” on page 31), double-click on the server and select the shared folder where your files reside. See Figure 17.

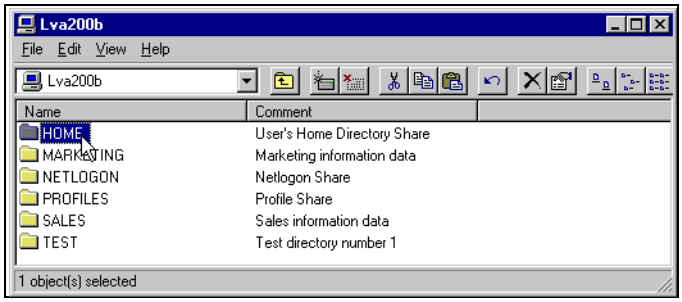


Figure 17. Shared resources on AIX Fast Connect server

or

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

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

   Where:

- `<ServerName>` is the NetBIOS name of the AIX Fast Connect server.
- `<SharedResource>` is the shared name.
- `[Path]` is the path where the files reside. See Figure 18 on page 36.

Figure 18. 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 in which 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 option **Map Network Drive** from the File menu.
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 19.

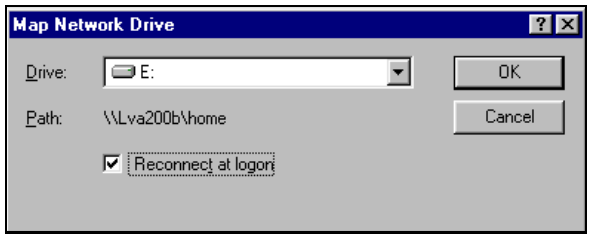


Figure 19. Map Network Drive

4.4.1.2 Command line interface

With the command line interface, the only way to access shared resources from AIX Fast Connect 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.

4.4.2 Accessing printer shares

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

There are two ways to configure a network printer in Windows 9x:

- Using the GUI interface
- Using the Command line interface

4.4.2.1 GUI interface

Perform the following steps to configure a network printer located in the AIX Fast Connect server:

1. Select the **Printers** administration folder by selecting **Start -> Settings -> Printer+s** or, alternatively, **My Computer -> Printers**.
2. Double-click the **Add Printer** icon to create a new printer. The Add Printer Wizard screen appears as shown in Figure 20.

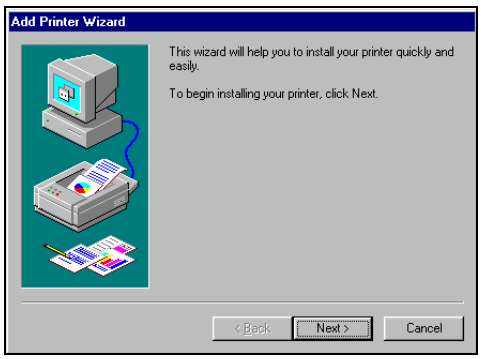


Figure 20. Add Printer Wizard

3. Press the **Next** button, and select the type of connection with the printer, in this case, a Network printer, as shown in Figure 21.

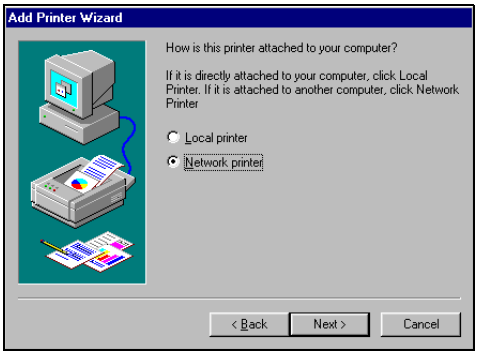


Figure 21. Select printer connection window wizard

4. Press the **Next** button, enter the network path where this printer is located (UNC), and select the **Yes** or **No** radio button option depending on whether you want to print from MS-DOS-based programs. See Figure 22.

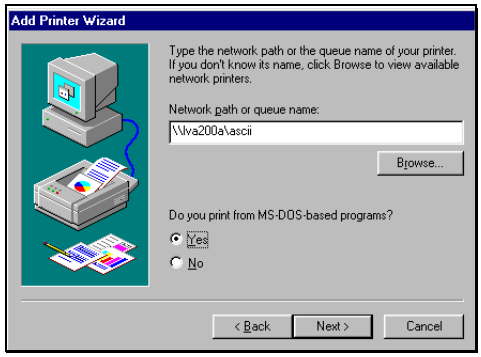


Figure 22. Enter the network printer path

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 23 on page 39.

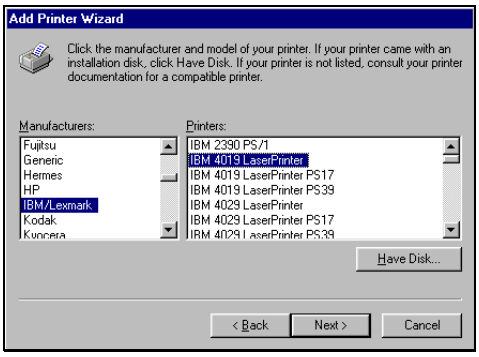


Figure 23. Select the printer driver window

6. Press **Next** button, and enter the printer name for your client as shown in Figure 24.

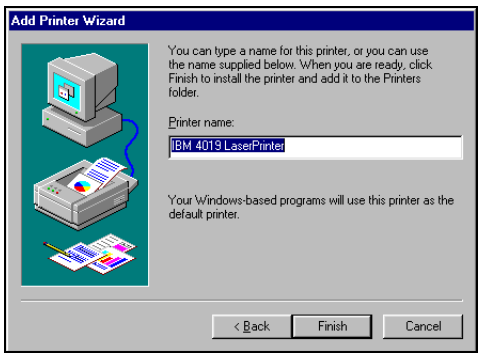


Figure 24. Set printer name window

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

4.4.2.2 Command line interface

To access a printer located on the AIX Fast Connect server from the command line, you must 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 Section 4.4.2.1, “GUI interface” on page 37, to associate a driver and a name to this printer.

Chapter 5. Accessing Fast Connect from Windows NT clients

This chapter will describe how to access shared resources, such as files and printers, from AIX Fast Connect server using Windows NT client.

5.1 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 25.

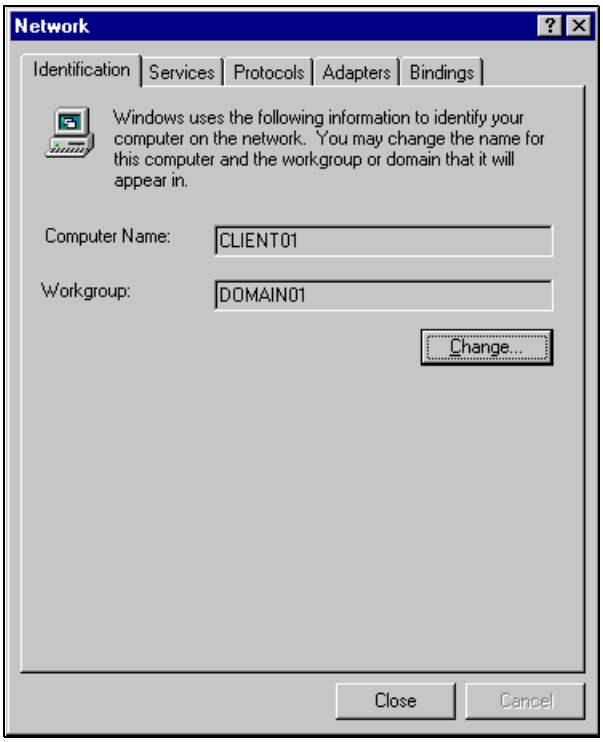


Figure 25. Windows NT Identification

While on the **Identification** tab, click the **Change** button, and you will see the dialog box shown in Figure 26 on page 42.

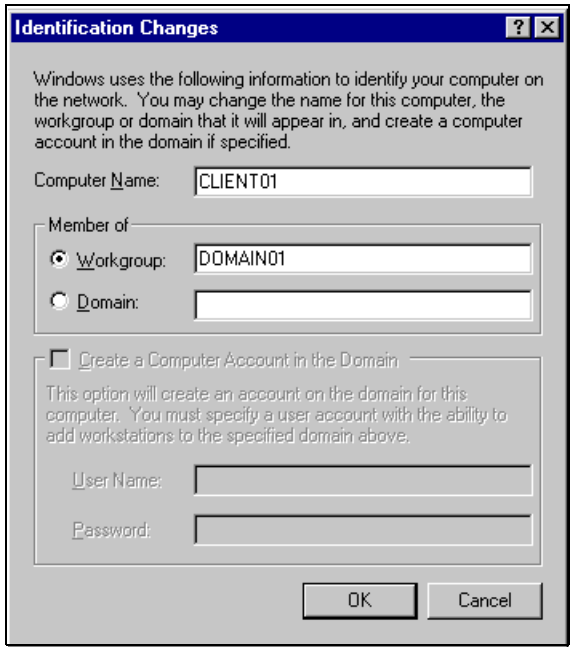


Figure 26. Identification Changes

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 must 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 Fast Connect server. You can make the Computer Name be the same name that you entered in your TCP/IP configuration. Click **OK** when finished.

You should now be back to the Network dialog box. If you have set up your Fast Connect server to provide NBNS 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 that shown in Figure 27 on page 43.

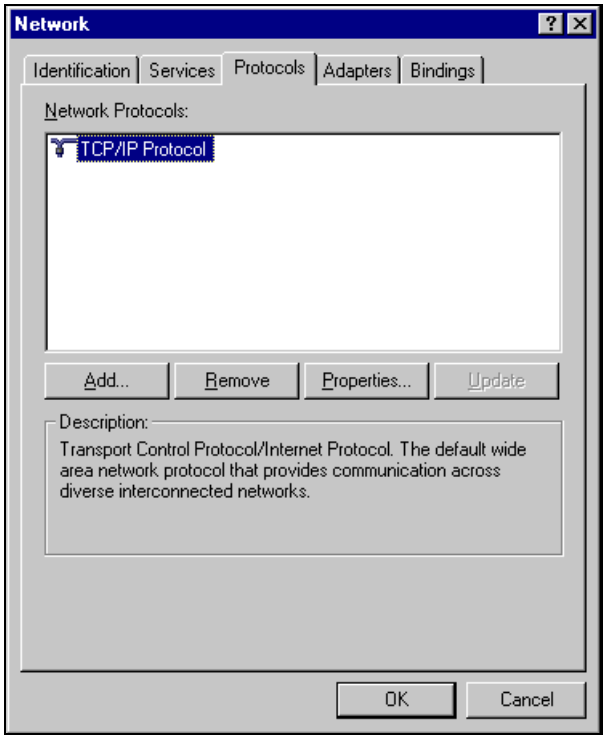


Figure 27. Protocols

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 28 on page 44.

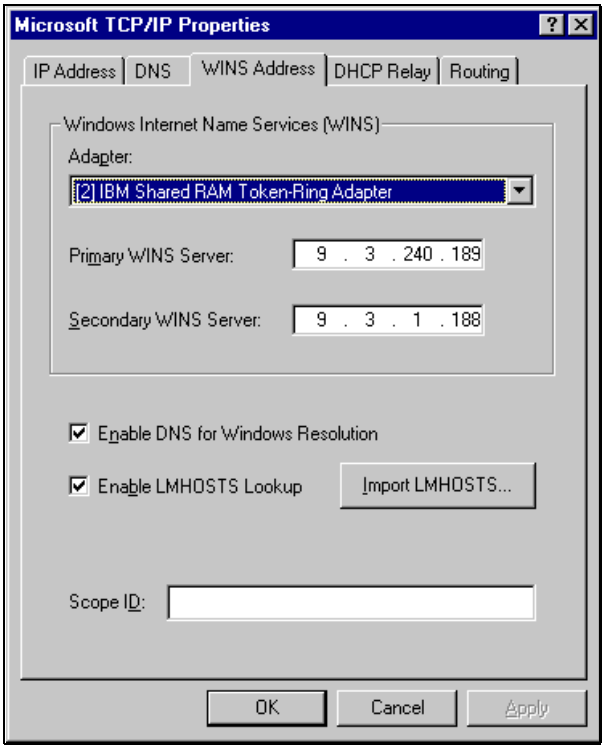


Figure 28. WINS Address

Enter the IP address of your Fast Connect 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, he or she 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 for the changes to take effect.

5.2 Locating the Fast Connect server

There are three ways to locate an AIX Fast Connect (FC) 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.

5.2.1 Locating the server through the Network Neighborhood icon

Perform the following steps to Locate the server through the Network Neighborhood icon:

1. double-click on Network Neighborhood icon
2. Double-click on Entire Network icon
3. Double-click on Microsoft Windows Network icon
4. Double-click on the domain of your Fast Connect server (see Figure 29)

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

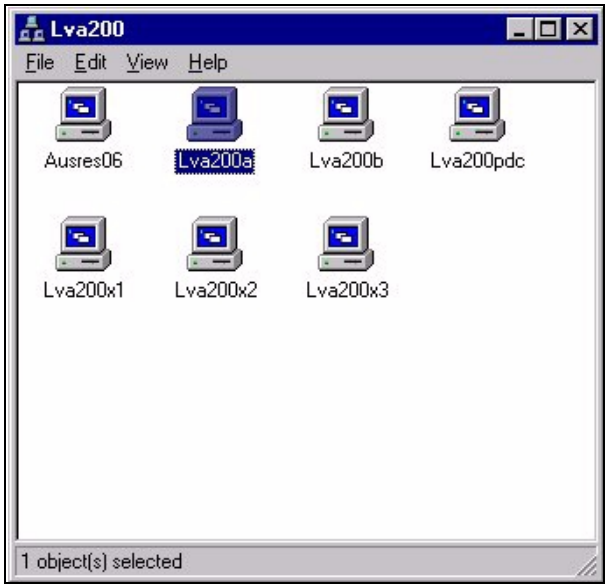


Figure 29. Browsing the LVA200 domain

5.2.2 Locating the server through the Find Computer option

You can use the **Find computer** option to find the Fast Connect server on the network. Perform the following steps:

1. Select **Start -> Find -> computer**.
2. Type the Computer Name (see Figure 30 on page 46).
3. Select **Find Now**.

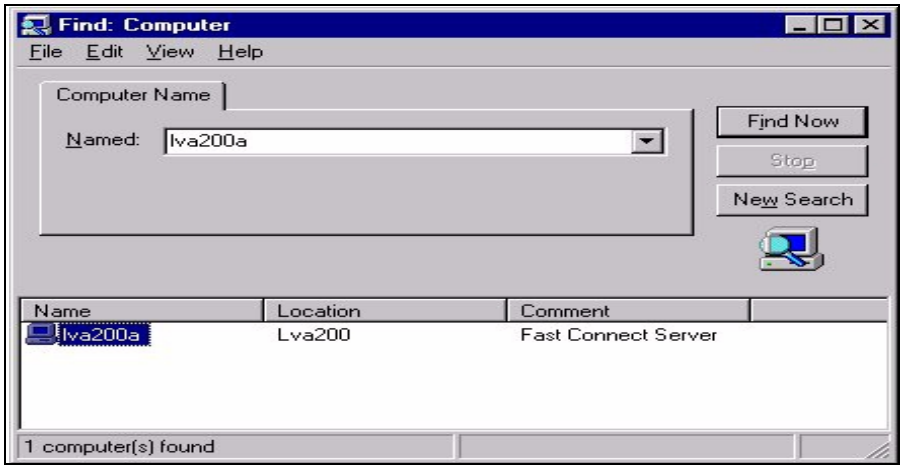


Figure 30. Find Computer

5.2.3 Locating the server from the command line

You can locate the AIX Fast Connect 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>` (where `servername` is the name of the Fast Connect server whose resources you want to view) or type
   `net view /DOMAIN:<domainname>` (where `domainname` is the name of the domain of your Fast Connect server). See Figure 31 on page 47.

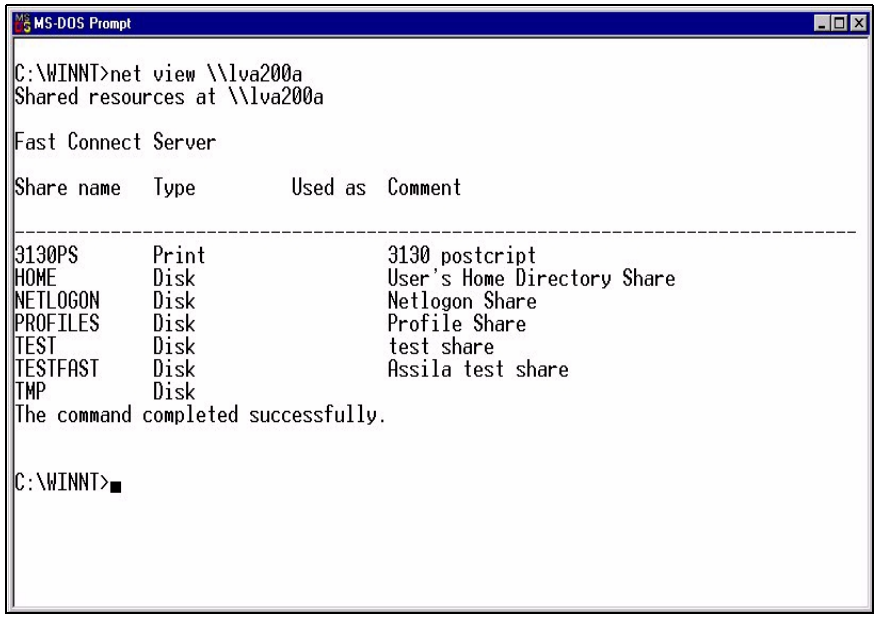


Figure 31. The net view screen

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.

5.3 Accessing resources from the Fast Connect server

The following sections describe how to connect Windows NT clients to the AIX Fast Connect server.

5.3.1 Accessing files

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

5.3.1.1 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. To do this, you can use the Network Neighborhood icon or the Find Computer panel.

In this example, we use the Find Computer option. You can perform the following steps to map a network drive to a Fast Connect shared resource:

1. Click **Start -> Find -> Computer**.
2. Enter the Computer Name and click on **Find Now** (see Figure 30 on page 46).
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).

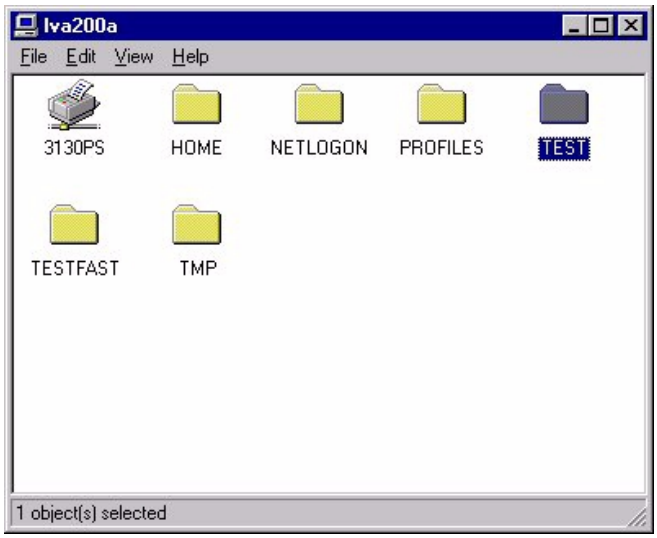


Figure 32. Fast Connect shares

5. Click on a shared resource, such as TEST, and select **File -> Map Network Drive..** or right-click on a shared resource and select **Map Network Drive..**.

6. Select the desired drive (for example, D:)
7. Click the **OK** button shown in Figure 33.

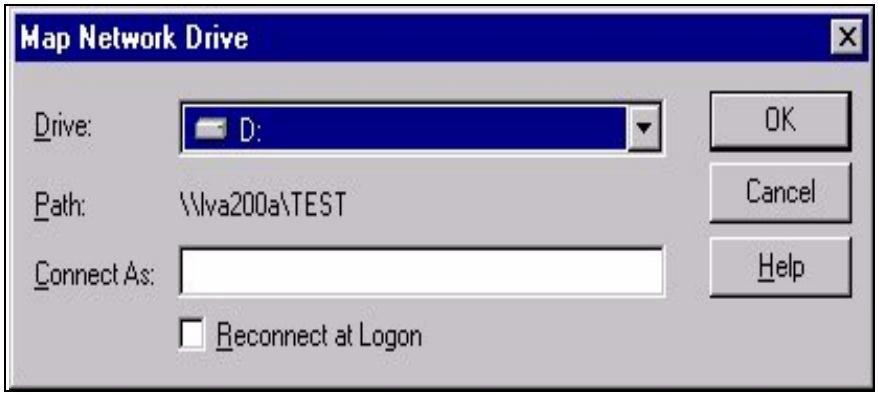


Figure 33. Map Network Drive

5.3.1.2 Command line interface

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

You have to use the `NET USE` command, as shown in Figure 34, to define mappings between PC drive letters and Fast Connect shared resources:

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

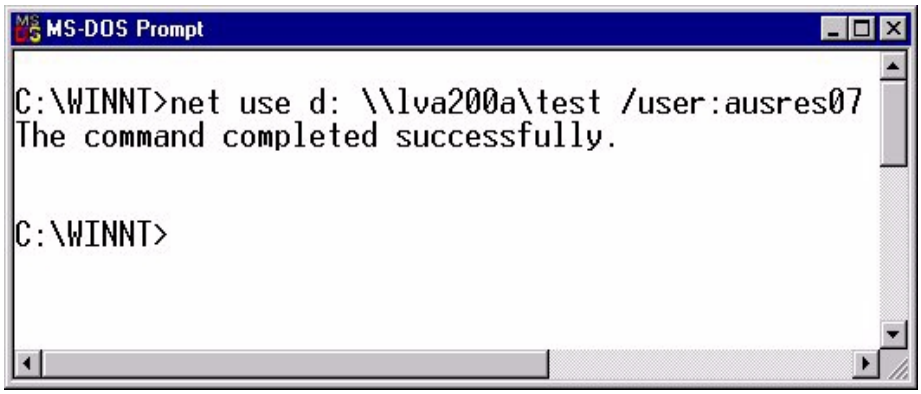


Figure 34. Map network drive from MS-DOS

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).

5.3.2 Accessing the AIX Fast Connect printers

If you want to access an AIX Fast Connect 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 of configuring a network printer on Windows NT:

- From the GUI interface
- From the command line interface

5.3.2.1 GUI interface

you can perform the following steps to configure a network printer from a 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). See Figure 35 on page 51.

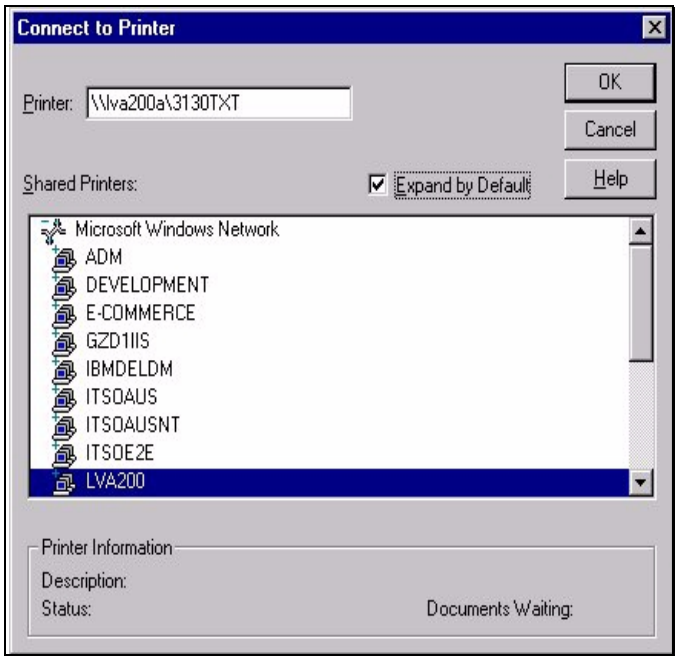


Figure 35. Connect to Printer

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 52.

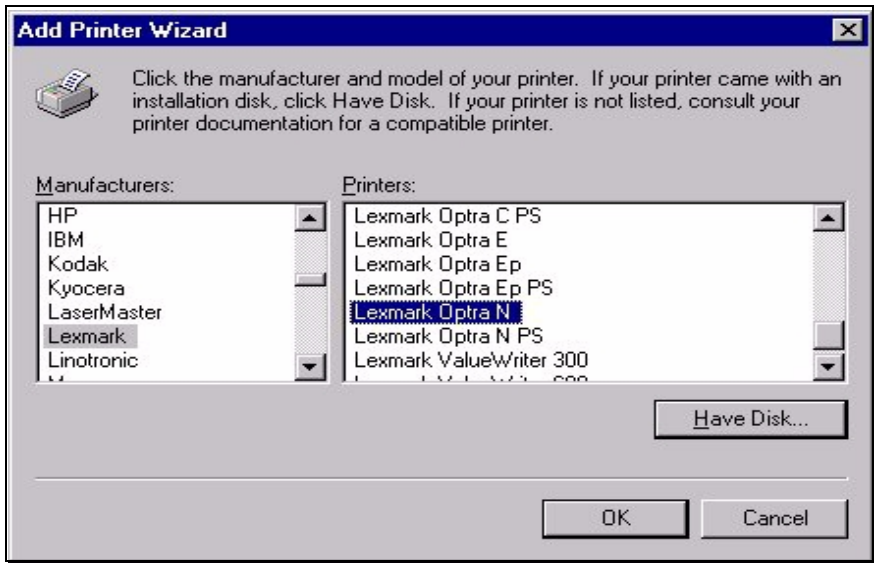


Figure 36. Select a printer driver from the Add Printer Wizard

5.3.2.2 Command line interface

For DOS application, you can map the network printer to local printer devices, such as 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. 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 53).

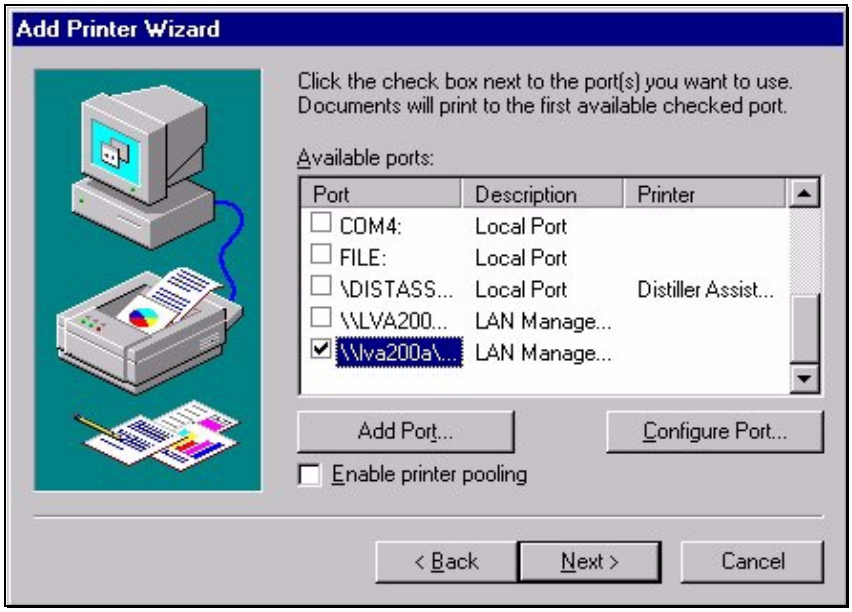


Figure 37. Selecting a port from the Add Printer Wizard

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 52).

Chapter 6. Accessing the Fast Connect server from Windows 2000

This chapter describes how to access shared resources, such as files and printers, from an AIX Fast Connect server using Windows 2000 clients.

6.1 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.

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

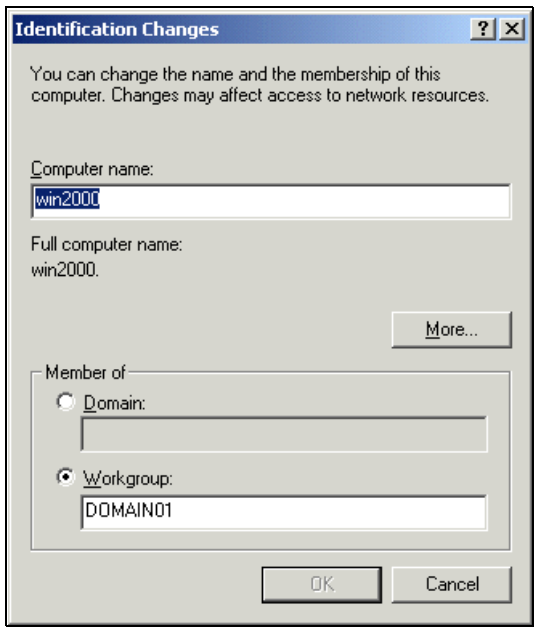


Figure 38. Identification Changes

You should enter your Computer name. Next, you have to click the **Workgroup** radio button and enter the workgroup name. The workgroup name should match the one you set up in your Fast Connect server.

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 all of the setup.

Return to the Control Panel and double-click **Network and Dial-up Connections**. Next, double-click the **Local Area Connection** icon. You should see the dialog box shown in Figure 39.

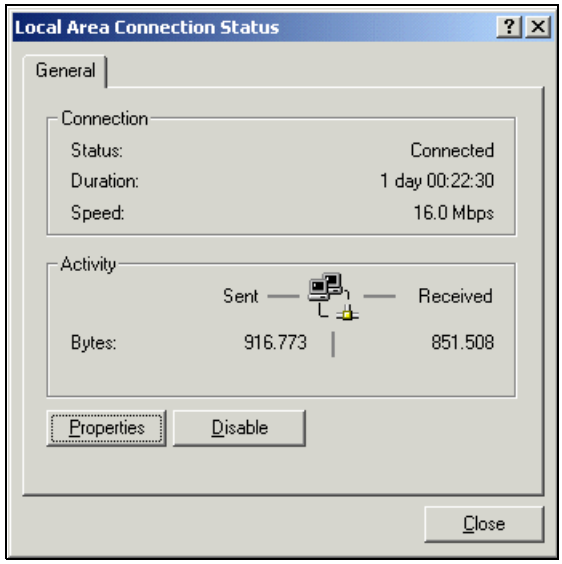


Figure 39. Local Area Connection Status

Click the **Properties** button, select **Internet Protocol (TCP/IP)**, and click **Properties**. You should see the Internet Protocol (TCP/IP) Properties dialog box as shown in Figure 40 on page 57.

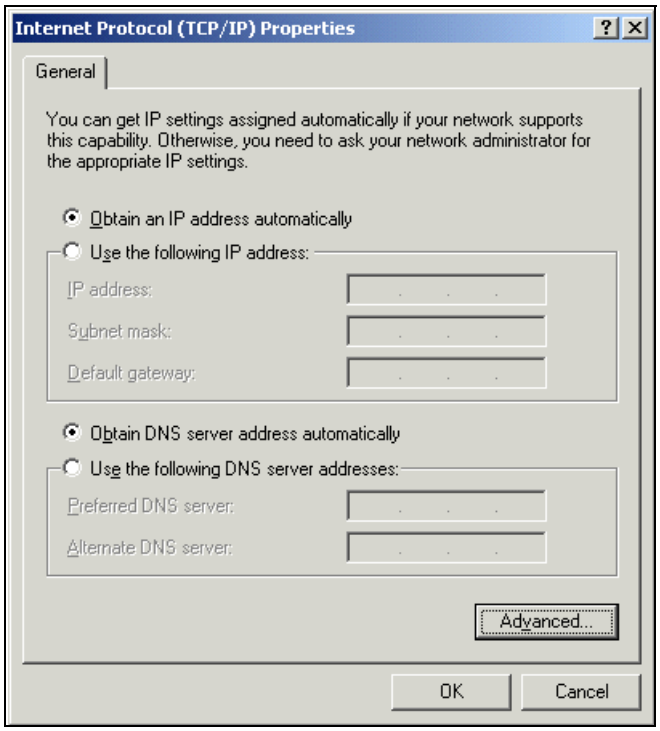


Figure 40. Internet Protocol (TCP/IP) Properties

Click the **Advanced** button. You should see the Advanced TCP/IP Settings dialog box. Next, select the **WINS** tab. You should see a screen like that shown in Figure 41 on page 58.

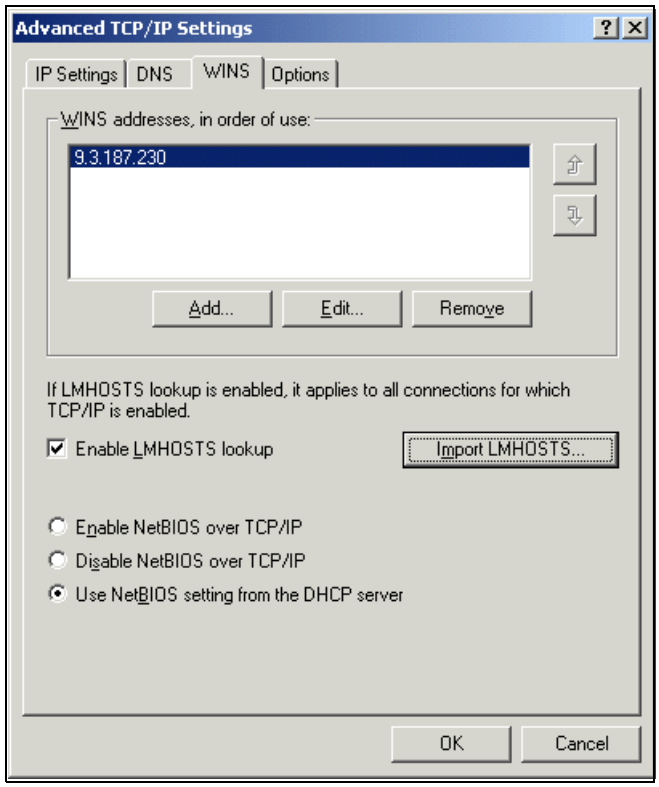


Figure 41. Advanced TCP/IP Settings

Click **Add**, and enter the IP address of your WINS server. If you have set up your Fast Connect server to provide WINS service, you can enter the IP address of your Fast Connect server in this field.

Now click **OK** in the Advanced TCP/IP settings dialog box, **OK** in the Internet Protocol (TCP/IP) Properties dialog box, **OK** in the Local Area Connection Properties, and **Close** in the Local Area Connection Status dialog box. You will need to reboot in order for the changes to take effect.

6.2 Locating the Fast Connect server

There are three ways to locate an AIX Fast Connect server from the 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.

6.2.1 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 Fast Connect server.

You will find the servers on the domain you have selected (see Figure 42).

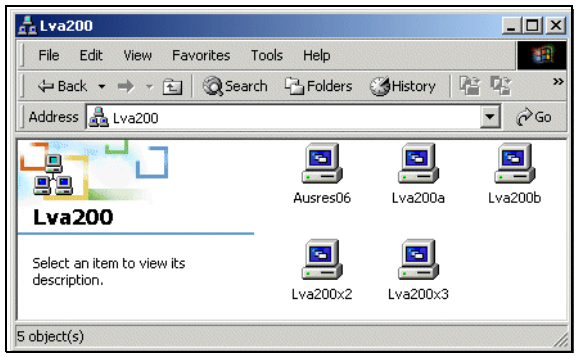


Figure 42. Browsing Lva200

6.2.2 Locating the server with the Search for Computer option

You can use the Find computer option to find the Fast Connect 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 43 on page 60).
5. Click the **Search Now button**.

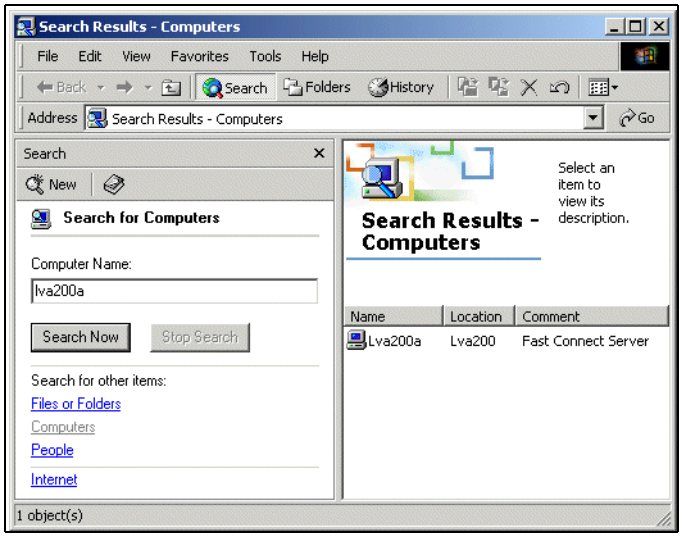


Figure 43. Search Results - Computers

6.2.3 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` is the name of the Fast Connect server whose resources you want to view), or type `net view /DOMAIN:<domainname>` (domainname is the name of the domain of your Fast Connect server). See Figure 44 on page 61.

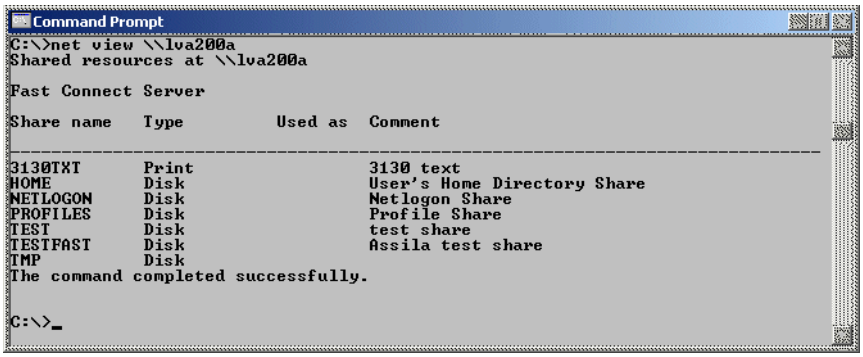


Figure 44. Net view screen

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, although that you can't view a list of workgroups.

6.3 Accessing resources from the Fast Connect server

The following sections describe how to connect a Windows 2000 client to an AIX Fast Connect server.

6.3.1 Accessing files

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

6.3.1.1 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 follow these steps to map a network drive to Fast Connect 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 43 on page 60).
5. Double-click the computer name (lva200a in this example).
6. You will see the shared resources of the lva200a server as shown in Figure 45.

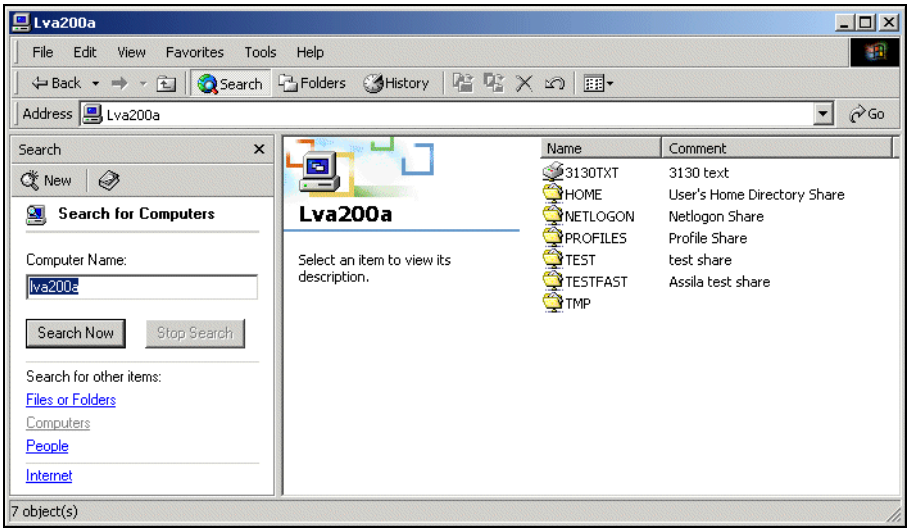


Figure 45. Fast Connect shared resources

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 **D:**).
9. Click the **Finish** button (see Figure 46 on page 63).

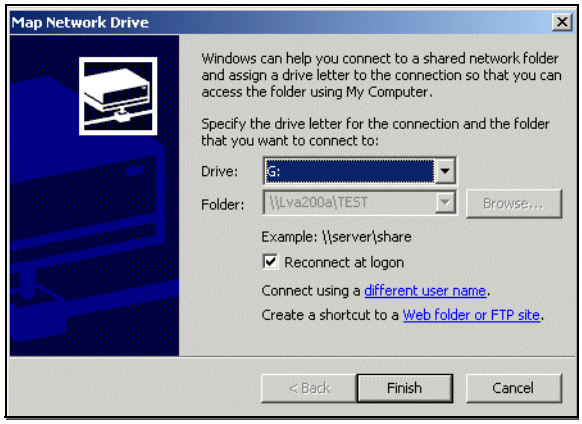


Figure 46. Map Network Drive

6.3.1.2 Using the command line interface

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

You have to use the `net use` command to define mappings between the PC drive letters and the Fast Connect 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
-------------------------------------------------------------------------------
```

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
-------------------------------------------------------------------------------
```

6.3.2 Accessing printers

If you want to access an AIX Fast Connect 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 the network printer on the Windows 2000 client:

- From the GUI interface
- From the command line interface

6.3.2.1 Using the GUI interface

Perform the following procedure to configure the 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 47 on page 65.

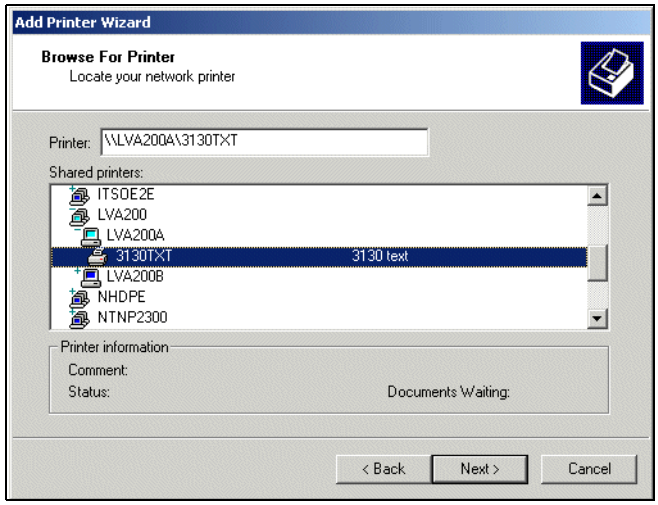


Figure 47. Connecting to a printer

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 48).

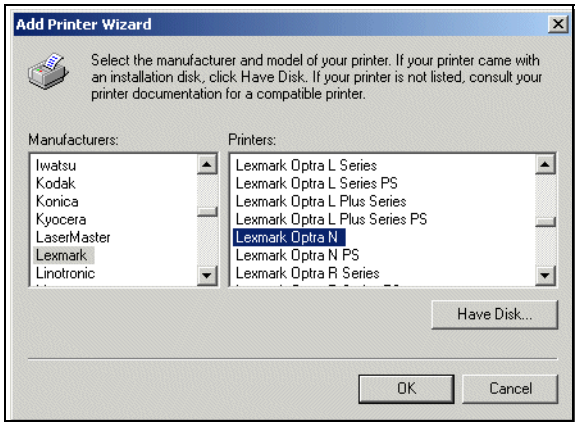


Figure 48. Add Printer Wizard

6.3.2.2 Command line interface

For a DOS application, you can map the network printer to local printer devices, such as LPT1. You can use the following simple device mapping on the 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 49), and press the **Next** button.

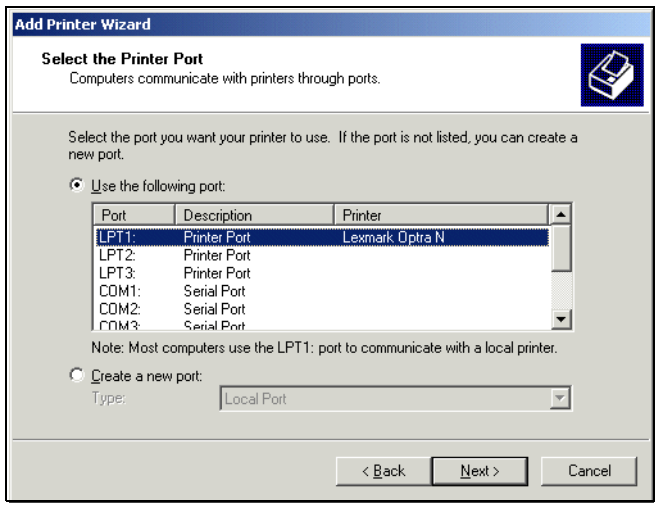


Figure 49. Selecting a port

5. Select the proper windows driver from the list (for example, select **Lexmark Optra N**), install it from the windows installation media (see Figure 48 on page 65), and press the **Next** button.
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.

Chapter 7. Accessing Fast Connect from OS/2 clients

This chapter describes how to access shared resources, such as files and printers, from an AIX Fast Connect server using OS/2 clients.

7.1 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 Fast Connect server on AIX. As part of the configuration, you will need to update both OS/2 Multiple Protocol Transport Services (MPTS) and LANRequester as part of this setup.

7.1.1 Configuring MPTS

The following steps 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**. This should produce the screen shown in Figure 50.

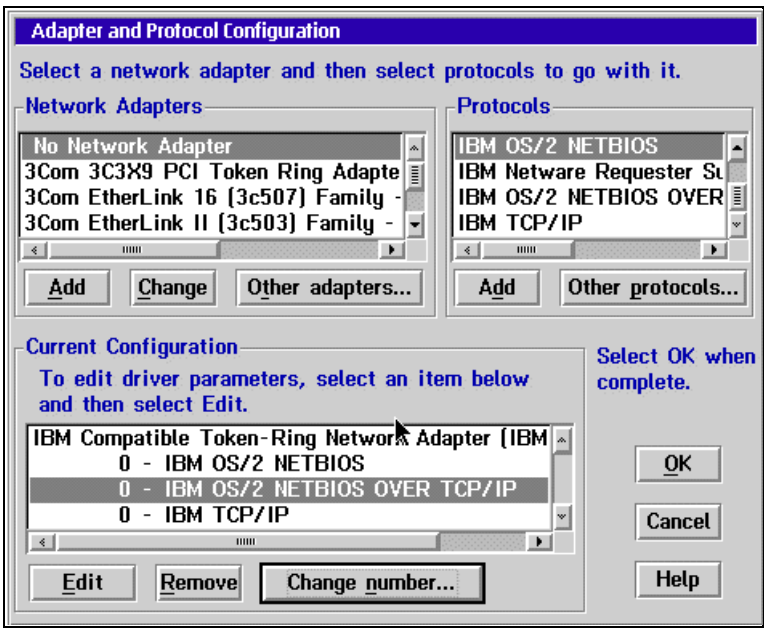


Figure 50. Adapter and Protocol Configuration

2. The current network adapter card and its protocols should be in the bottom left-hand corner of the dialog box. You will need to select **IBM OS/2 NETBIOS OVER TCP/IP** in the upper right-hand 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 51.

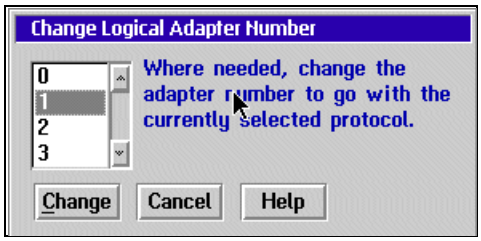


Figure 51. Change Logical Adapter Number

4. Now, you have to change the logical adapter number. You can choose the number 1 (if it is available) and click **Change**.
5. Now, you should see the dialog box, shown in Figure 52 on page 69, with a new number for your logical adapter.

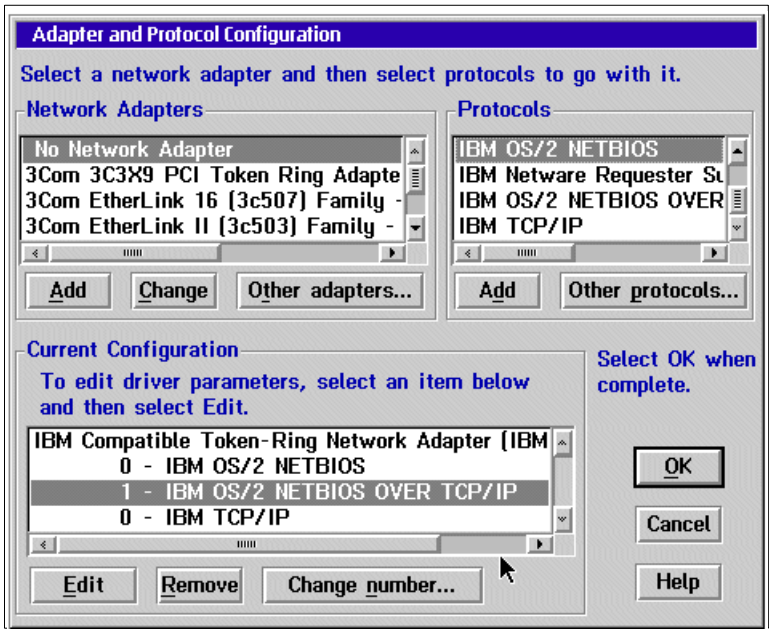


Figure 52. New logical adapter number

7.1.2 Modifying the RFCNAMES file in OS/2

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

1. Double-click on **IBM OS/2 NETBIOS OVER TCP/IP**. This should produce the screen shown in Figure 53 on page 70.

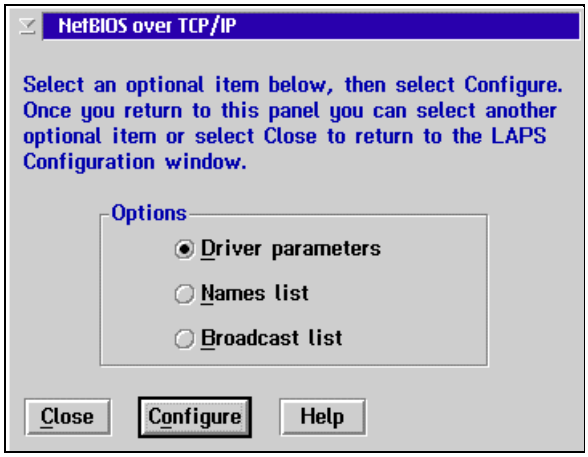


Figure 53. NetBIOS over TCP/IP

2. Select **Driver parameters** and click **Configure**. You will see the dialog box shown in Figure 54.

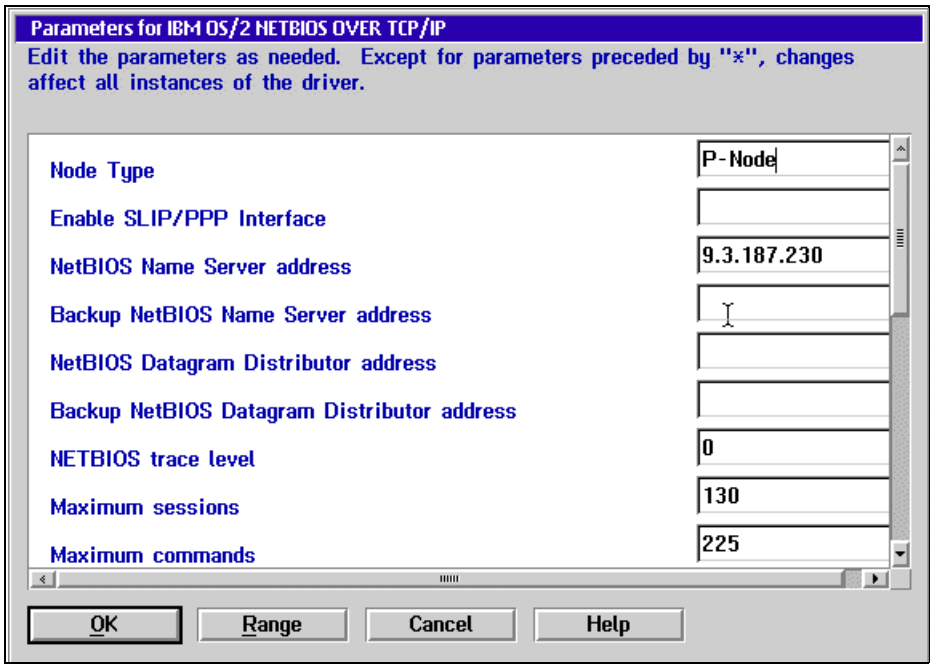


Figure 54. Parameters for IBM OS/2 NETBIOS OVER TCP/IP

- Change the Node Type field to **P-Node**.
- Enter in the NetBIOS Name Server address the IP Address of your name server. If you configured your Fast Connect server with WINS support you can enter here the IP address for you Fast Connect server.
- 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 55.

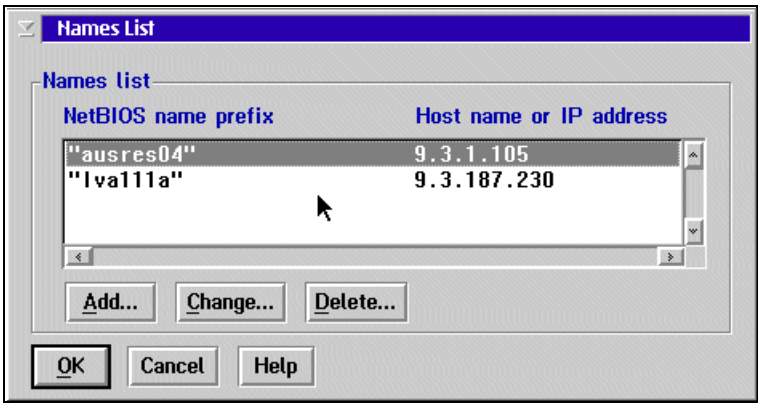


Figure 55. Names List

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

7.1.3 Configuring 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 shown in Figure 56 on page 72. Select **Easy**.

Figure 56. Easy or Tailored Installation/Configuration

5. You will see the dialog box shown in Figure 57. Select **Change LAN names**, and click **OK**.

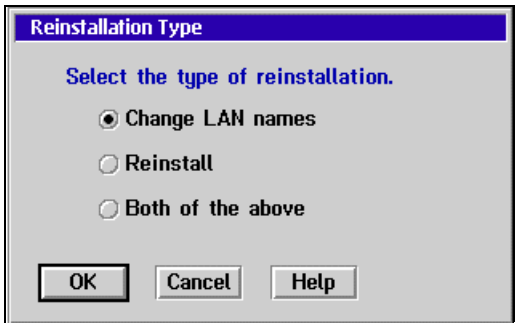


Figure 57. Reinstallation Type

6. On the next screen, shown in Figure 58, you need to enter the name of the computer. Next, click **OK**, and you will see the dialog box shown in Figure 59 on page 73.

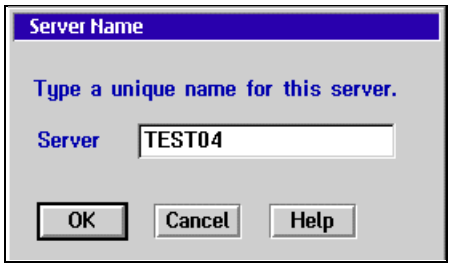


Figure 58. Server Name

7. 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 Fast Connect server.

Figure 59. 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 Installation/Configuration Completed dialog box. Click **OK**.

7.1.4 Verifying the configuration

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

7.1.4.1 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 the following:

```
wrknets = net1,net2
```

7.1.4.2 PROTOCOL.INI

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

```
[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
```

Shut down and restart the system to pick up the changes.

7.1.4.3 Obtaining a share resource

Here are a few helpful hints to remember when you want to obtain a share resource from the Fast Connect server on an OS/2 client:

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

Below, you can see some examples of how to access a shared resource.

~~~
[<test04>-C:\]net view \\lva111a
Shared resources at \\lva111a
Fast Connect 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.
~~~

You can use the `net view` command, as shown above, to see which resources are available. 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:\]
~~~

Chapter 8. Fast Connect advanced functions

The Fast Connect product offers some additional functions that can help us answer special requirements and improve overall performance.

8.1 Unicode

The Fast Connect server represents shares, users, files, and directory names internally using Unicode. That means that there is no problem displaying different characters for the non-English languages if a client also supports Unicode.

You must ensure that you have the Unicode feature installed on the AIX server. This is done by installing the corresponding fileset and setting the appropriate language environment. Your current language setting is specified by the LANG environment variable:

```
$ print $LANG
en_US
```

If, for example, you use the en_US language (ISO8859-1), you should change it to the EN_US language (UTF-8). You can do this with the SMIT or the Web-based System Manager. Use the `mle_cc_set_hdr` fastpath with the first one. If you use WebSM, select the **System** icon and then the **Cultural Environment** icon.

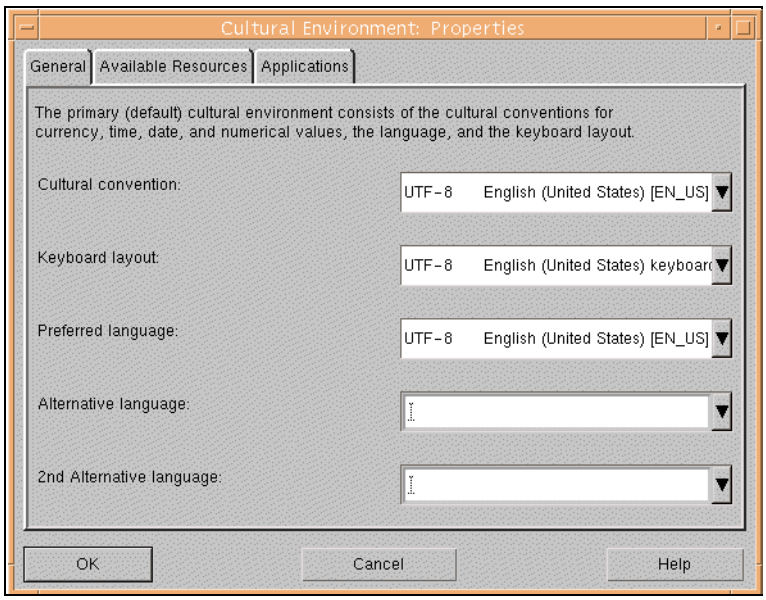


Figure 60. Setting the cultural environment

Clients who use Windows 95 or other clients who do not support the Unicode must ensure that the client and server locales match.

8.2 Support for Access Control Lists

The Fast Connect server supports the AIX Access Control Lists (ACL). Be careful; even if the name is identical, it is not the same as the Windows ACL. Normal UNIX access control is limited to specifying read/write/execute permissions for the owner, group, and other users. You have more control over a file access with the ACL. You can specify the file permissions, based on a user name or his/her group. You can read more about the ACL in the AIX documentation *AIX Version 4 System Management Guide: Operating System and Devices*, SC23-2525

You can see files that are ACL-enabled if you list them with an -e option. Files with the ACL will have a plus sign (+) in the eleventh column. Here is an example of such a listing where you can see one directory (.) and one file (test.txt) with enabled ACL information:

```
lva200c>root$ ls -ela
total 42587
drwxr-xr-x+  18 ausres06 staff       1024 Feb 14 23:42 .
drwxr-xr-x-2356 bin      bin        44032 Feb 09 17:37 ..
-rwxr--r-x-   1 ausres06 staff        476 Feb 02 13:07 .kshrc
-rw-r--r---   1 ausres06 staff        325 Feb 08 14:05 .profile
-rwxr-xr-x+   1 ausres06 staff          0 Feb 14 23:44 test.txt
```

You have two ways to change this ACL file information:

- With the `acledit` command
- With the graphical editor in CDE

8.2.1 Editing ACL information with the acledit command

You can set the ACL information for the file or directory with the `acledit` command. Before using it, check that you have defined the EDITOR variable with the full path of the editor:

```
export EDITOR=/usr/bin/vi
```

When you run the `acledit` command, you will see the basic and extended file permissions in the selected editor. You can modify them, save the file, and exit. Answer **yes** to the question about applying modified ACL. Here is an example of file permissions:

```
attributes:
base permissions
    owner(ausres06):  rwx
    group(staff):  rwx
    others:  r-x
extended permissions
    enabled
    deny rwx u:ausres07
~
~
"/tmp/acledit.72730/acle.dhbEa" 8 lines, 157 characters
```

The user, ausres07, could modify the file before ACL extended permissions were applied but not after, as you can see in the following example:

```
# su - ausres06 -c "print test >/tmp/test.txt"
# su - ausres07 -c "more /tmp/test.txt"
# export EDITOR=/usr/bin/vi; acledit /tmp/test.txt

su - ausres07 -c "more /tmp/test.txt"
/tmp/test.txt: The file access permissions do not allow the specified action.
#
```

8.2.2 Editing ACL information within the CDE

You can use the graphical editor to specify or change ACL permissions in CDE. The editor's name is dtacljfs and it accepts files as parameters. For example,

```
dtacljfs /home/ausres06/.profile
```

would open a window, such as the one shown in Figure 61.

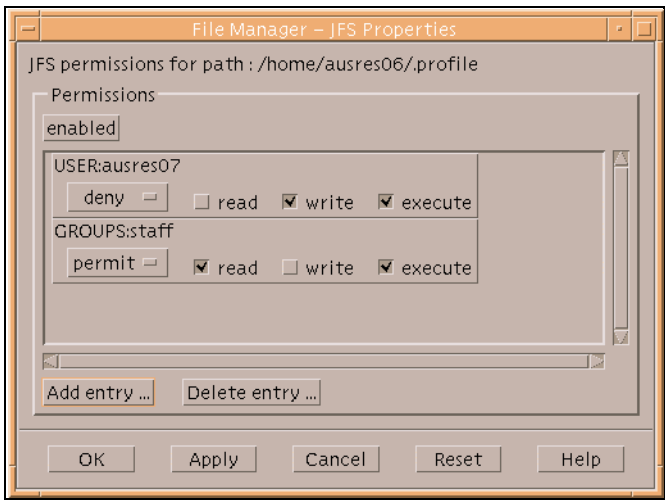


Figure 61. Editing ACL permissions in CDE

You can then use this utility to enable/disable and add/remove the ACL extended permissions for the file.

You can use this editor inside the File Manager if you modify the /usr/dt/config/en_US/dtfile.config or the dtfile.config corresponding to your own locale. Locate the line

```
#aix:3      = jfs
```

and uncomment it (remove the first character - '#'). Then, restart the Workspace Manager.

You can access file permissions in the File Manager if you select a file, click the right mouse button, and select the **Change Permissions...** option. The File permissions window will open, and you will see the additional button, Change JFS ACL as shown in Figure 62. If you press this button, you will come into the dtacljfs editor.

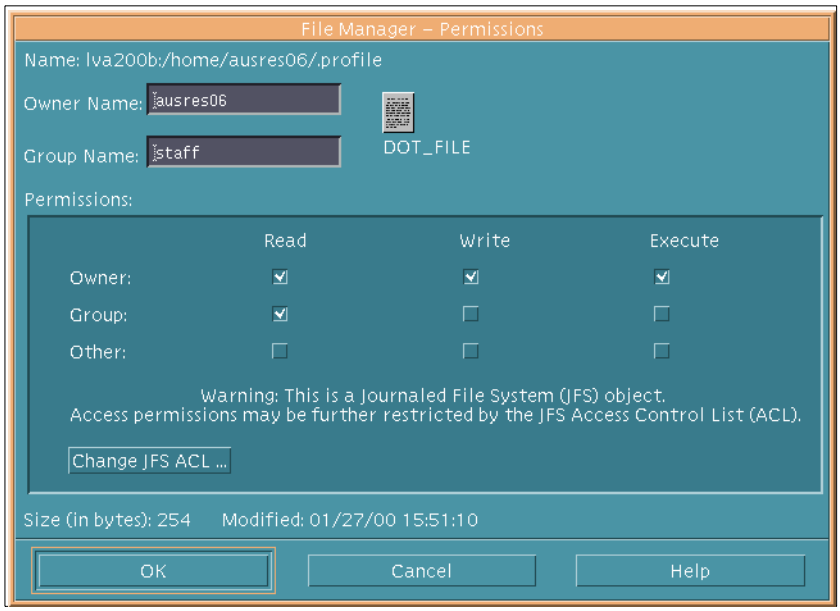


Figure 62. File Manager permissions editor with Change ACL button

8.2.3 ACL inheritance

The Fast Connect server also implements the ACL inheritance (it is not an AIX ACL functionality). That means that the files created with the Fast Connect server will inherit the ACL settings of the user's home directory. You can reduce your ACL administrative work with this feature offered by the Fast Connect server.

You must specify the ACL inheritance in the /etc/cifs/cifsConfig file. Locate the line with the string, acl_inheritance, and change the value to 1. You must restart the server after this change to the configuration file.

8.3 File locking

The file server must use the file locking for operations on files. This assures that, for example, two users are not writing to the same file at the same time. The Fast Connect server implements an option to work with the opportunistic locks (oplocks). This is an advanced type of locking, which can significantly improve network performance.

With the oplocks, a client has a mechanism with which to buffer file data locally. One possible scenario is with the data write. The data can be buffered locally if a client knows that no other client is accessing the data. The second possibility is when reading the data. The client can buffer read-ahead data if no other client is writing the data.

The CIFS protocol defines three types of oplocks:

exclusive oplocks Allows the client to open a file for exclusive access and allows a client to perform arbitrary buffering

batch oplocks Allows the client to keep a file open on the server even though the client application has closed the file

level II oplocks Indicates that there are multiple readers of a file and no writers

The Fast Connect server supports the first two types of oplocks.

Note

If you access the same files both from the AIX and from the clients at the same time, you must disable this opportunistic locking, since the oplocks mechanism is implemented within the Fast Connect server, and doesn't check the AIX accesses.

You can set the oplock policy by modifying the configuration file, /etc/cifsConfig, where you can set two options:

oplockfiles = [yes|no] Enable/disable use of the opportunistic locking mechanism. If oplocks are not active, the server is using a byte range SMB locking.

oplocktimeout = time Define oplock time-out value in seconds. This value is used when the server tries to break locks and send break message to a client. If the client does not respond in this time-out period, it is declared *dead* and locks on the file are released.

8.4 Send File API support

The Fast Connect server supports the TCP/IP Sendfile API (application programming interface) support. This is an in-kernel network file cache to improve TCP/IP performance.

Sendfile setting is done with the `net config` command. You can use the following options:

/send_file_api:0|1 Disable/enable the Sendfile API.Default value is 1.

/send_file_size:val Defines an SMB read size limit, where the server will use the Sendfile API. If an SMB read size is greater than this parameter value, Sendfile API will be used for this SMB read operation. The default value is 4096.

/send_file_cache_size:val Defines an SMB read size limit where the server will cache the file. If an SMB read size is smaller than this parameter's value, Sendfile API will cache the file. The default value is 0 and this means that the Sendfile API will cache any file.

There is one additional parameter in AIX that can be set to tune the Sendfile API performance. It is set with the `no` command:

send_file_duration Specifies the cache validation duration for all the file objects that the system call send_file accessed in the Network Buffer Cache. This attribute is expressed in seconds; the default is 300.

In the following example, we will enable the Sendfile API and reduce the cache validation time to one minute (60 seconds).

```
# net config /send_file_api:1
# no -o send_file_duration=60
```

8.5 Mapping file names

The mapping of file names from Windows 95/98/NT to AIX Fast Connect server and back normally works without problems. But, there are special cases when we must be more careful. Two possible problems can arise when you work with the same file from an AIX and Windows client.

8.5.1 Differences in character casing

Windows does not distinguish between upper- and lower-case characters in a file name; so, the file names, MyFile.txt and myfile.txt, both define the same file. On the other hand, AIX treats these two file names as two different files. The problem can only arise when you create such files directly on AIX and use them on a Windows client. In this case, some functions will work and some will not.

An example of unexpected behavior is when you create two files in an AIX directory that is also an AIX Fast Connect share.

```
$ print "small" >longfilename.txt
$ print "BIG" >LongFileName.txt
```

You can now see two different files in Windows NT Explorer and you can work with them without any problems, but, from the command prompt, you will get the same output from two files:

```
C:\> type longfilename.txt
small

C:\> type LongFileName.txt
small
```

You should avoid creating file names that differ only in their casing in shared directories on AIX.

8.5.2 Mapping AIX long file names to DOS file names

Old Windows clients, such as Windows 3.11, do not support long file names. This restriction requires the mapping of long AIX file names (AFN) to DOS file names (DFN). Truncation of names is not enough, because two different long file names can be represented as only one DOS name.

The Fast Connect server uses the Windows NT method for mapping from AFN to DFN that ensures file name uniqueness. This method uses a delimiter character in a short name followed by a unique number (for example, the AIX_Fast_Connect_Server file name would be converted to AIX_FA~1). The mapped name is generated whenever the AFN needs to be passed back to a Windows client.

Mappings from AFN to DFN are consistent during the lifetime of the Fast Connect server. You lose this mapping when the server restarts. For example,

consider two files in an exported share, LongFileNameX.txt and LongFileNameY.txt. Client, that look at the share. They would see

LONGFI~1.txt for LongFileNameTrue.txt

and

LONGFI~2.txt for LongFileNameFalse.txt

You want to edit LongFileNameTrue.txt; so, you open the file, LONGFI~1.txt, on the client. After changing, save and close the file. Then, the server shuts down and somebody (re)moves your file, LONGFI~1.txt, from the file system. Once the server is up and running, you once again open LONGFI~1.txt, and, this time, LONGFI~1.txt will map to LongFileNameFalse.txt! Therefore, if the network drive is reconnected following server restart, a new file list must be obtained before accessing any mapped names.

You can modify AFN to DFN mapping with the `net` command:

`net config /listparm /component:smbserver /parameter:dosfilenamemapping`
Shows the current setting for long file name mapping

`net config /component:smbserver /dosfilenamemapping:[0|1]`
Changes the long file name file mapping on/off

`net config /listparm /component:smbserver /parameter:dosfilenamemapchar`
shows the current delimiter character for long file name mapping. You can select only between `~` and ^.

`net config /component:smbserver /dosfilenamemapchar:[~|^]`
Changes the delimiter character for long file name file mapping

8.5.3 DOS file attributes

You might want to decide and map DOS file attributes, such as System, Hidden, and Archive to the AIX files permission. The method to do that is to modify the dosattrmapping parameter in the /etc/cifs/cifsConfig file.

If this parameter is set to 1, the Archive, System, and Hidden attributes are mapped to User, Group, and Other execute bits. Otherwise, these attributes are not supported. This is only valid for files.

8.6 Guest Logon Support

Fast Connect can support guest-mode logins when configured for either plain-text or encrypted passwords. (Guest mode is not supported if Fast Connect is configured for NT-passthrough authentication, DCE/DFS

authentication.) To enable guest-mode logins, two parameters must be configured:

net config /guestlogonsupport:1 (enables guest logons)

net config /guestname:GuestID (AIX guestid with null password)

When Guest Logon Support is enabled (guestlogonsupport=1), and the guestname field is set, non-AIX users can connect to the Fast Connect Server. The credentials for these guest clients will be set to those of the guestname attribute.

The AIX account specified by guestname must have a null AIX password. It is being used for guest-mode access to the AIX file system. This guest account will be able to access all of the file system directories exported by Fast Connect (as File Shares). Therefore, to simplify access-control, this guest account should probably be in its own unique AIX-group.

Guest access is only given to Usernames that are not standard Fast Connect users, with Passwords that are not null.

Incoming login-requests are authenticated as follows:

1. If the incoming Username is recognized as a Fast Connect user, the password is checked. If the Password is valid, standard user-mode access is granted; otherwise, the login-attempt fails.
2. If the incoming Username is not recognized as a Fast Connect user, the Password is checked. If the Password is non-null, guest-mode access is granted; otherwise, the login-attempt fails.

When Guest Logon Support and encrypted passwords are both enabled, the guestname user does not have to be added to the Fast Connect user database (/etc/cifs/cifsPasswd) but is still required to have a NULL AIX-password.

Guest Logon Support does cooperate with Network Logon support (networklogon=1). Whenever guest-mode access is granted, the profile, startup scripts, and home directory of the guestname user will be used for the network logon.

If dce_auth=1, Guest Logon Support does not work.

If passthrough authentication is configured, Guest Logon Support does not work.

To disable Guest Logon Support, type `net config /guestlogonsupport:0`.

8.7 Alias names support

The AIX Fast Connect product supports server name aliases. You can use this in high-availability configurations of the Fast Connect server (HACMP mutual takeover). You can configure aliases with the `net name` command. The following options are available:

`/add <alias> [/sub:<val>]`

add new alias for the Fast Connect server NetBIOS name. /sub defines the NetBIOS name subcode, with values form 00 to FF in hex. If you do not specify sub value or you specify 00 or 20, both 00 and 20 subcodes aliases will be added for that NetBIOS name. You cannot add an alias if someone on the subnet is holding it. If nobody on the subnet is holding the alias name but it exists in the WINS or NBNS, the alias name will only be added to the local name table:

`/delete <alias> [/sub:<val>]`

Delete the defined alias for the Fast Connect server NetBIOS name. /sub defines the NetBIOS name subcode, with values from 00 to FF in hex. If you do not specify a sub value or you specify 00 or 20, both 00 and 20 subcodes aliases will be deleted for that NetBIOS name:

`/list`

List all aliases for the Fast Connect server NetBIOS name. The subcode for the alias is listed after the name between < and >, unless the alias subcode is 00 and/or 20.

All NetBIOS name aliases will be registered to the WINS or NBNS server if the primary or secondary address of the server is specified in the Fast Connect configuration.

8.8 Accessing DFS directories

Fast Connect 2.1.1 introduces a new feature: The ability to export DFS directories. This section explains how to set up AIX and Fast Connect to allow the clients connected on the PC workstations to access DFS directories. There are two ways to perform this operation.

8.8.1 Global access to Fast Connect

With this first method, you set up Fast Connect so that every connection forces an authentication of the users and passwords within the DCE environment.

8.8.1.1 Setup of Fast Connect

The setup of Fast Connect uses the usual menus. Figure 63 shows the attribute to modify to authorize DFS access.

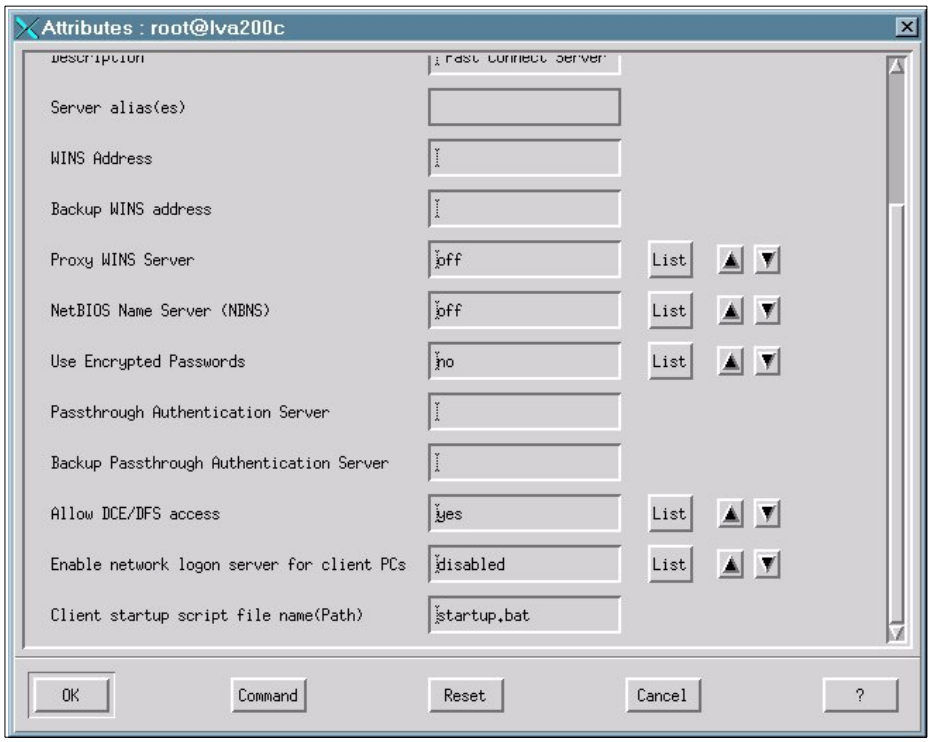


Figure 63. Authorizing DFS access

There are two attributes that are important to allow DFS access:

- Allow DFS access must be set to YES.
- Use Encrypted passwords must be set to NO.

The export of a DFS directory is not much different from the export of a regular directory, except, perhaps, for the use of the : shortcut as shown in Figure 64 on page 89.

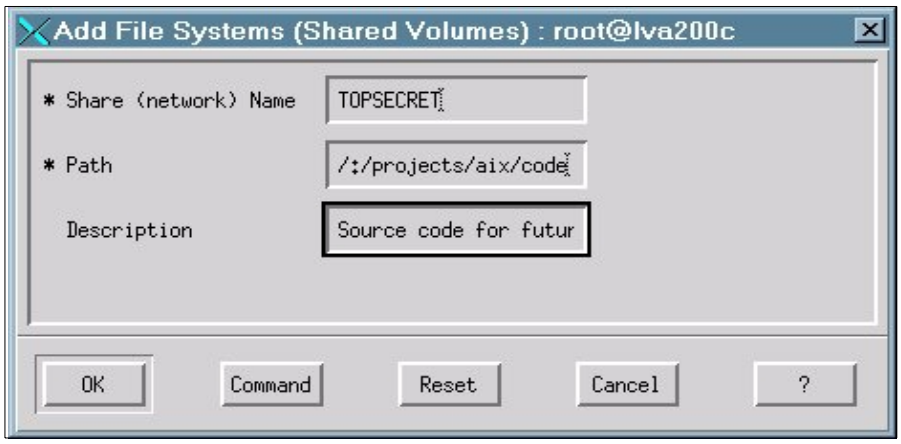


Figure 64. Exporting a DFS directory

8.8.2 Fast Connect DFS access mechanism

You should use this method if all the clients have a DCE logon. There is no local authentication; so, any client not having a DCE login but just a local user and password on the AIX machine will not be able to log on. The default HOME share is being modified as well. Instead of the local home directory, the HOME share is now the DCE home directory. The user identifier and group identifier used directory are the DCE ones. you should synchronize the local user identifier with the DCE one to avoid conflicts.

Let us consider a worst-case scenario. You have set up Fast Connect to allow users to access DFS. You have a Windows user, named matt, with the local AIX user name, fox, a local identifier of 201, a DCE user name of matt, and a DCE identifier of 6401. You also have another user on the local system with the user name, bob, and a local user identifier of 6401. The Windows user, matt, can map his DCE home directory by providing *matt* as a user name plus his DCE password. However, if this user wants to map a local share, let us say, TEMP (a share that contains the /tmp/directory), every file and folder that matt will create will have the user identifier, 6401, and the local owner of those files will be bob.

To avoid this problem, make sure that the local and DCE identifier and names of your users are synchronized.

8.8.3 Using the AIX integrated login

The previous methods simplify the administration of the users since everything can be done centrally. But, what if not all the users have a DCE account and you want just some of them to be able to access their DCE home directories. Using the AIX integrated login can be the answer to this question.

The AIX integrated login is a feature that allows you to modify the login mechanism to bundle the login in the DCE environment with the original AIX login. Refer to the DCE documentation for a complete description of this feature. In a simple environment, installing this integrated login can be summarized by the following steps:

1. Synchronize user names and identifier.
2. Modify the /etc/security/user file, and add a stanza, SYSTEM = dce, for the users that need to access DFS.
3. Synchronize the password between the DCE and the local environment.

The situation you have now, is this:

- The users that do not have an integrated login can log using the local environment and will be able to access the local share and the DFS shares as if they where a member of the any_other group.
- The users that have an integrated login can log to the local shares but also to the DFS shares that they are allowed to access with their DCE identifier.

Chapter 9. Authentications models

This chapter describes the authentication methods supported by an AIX Fast Connect server to improve the management and security of the system. An AIX Fast Connect server can use different methods to validate users and give them access to shared resources, such as file directories and printers.

AIX Fast Connect can handle both the DES encryption method used on AIX and the RSA MD4 encryption algorithm used on Windows systems. In this chapter, we will cover the differents ways of configuring AIX Fast Connect to use the various authentication methods supported (non-encryption, encryption, mixed, and passthrough).

9.1 Using AIX Fast Connect server with non-encrypted passwords

When the AIX Fast Connect sever is installed, the encrypted password option is disabled. The reason for this is to satisfy the configurations where it is necessary to maintain the compatibility. It is only necessary to keep a unique database for the users and passwords in AIX. The user database used by AIX is located in the /etc/passwd file, and the encrypted passwords database using the DES encryption method is located in the /etc/security/passwd file. With this configuration, the passwords are sent through the network as clear text, and it is a security risk because any user monitoring the network could find out users' passwords.

The flow chart, shown in Figure 65, illustrates the authentication process when the non-encryption option is disabled.

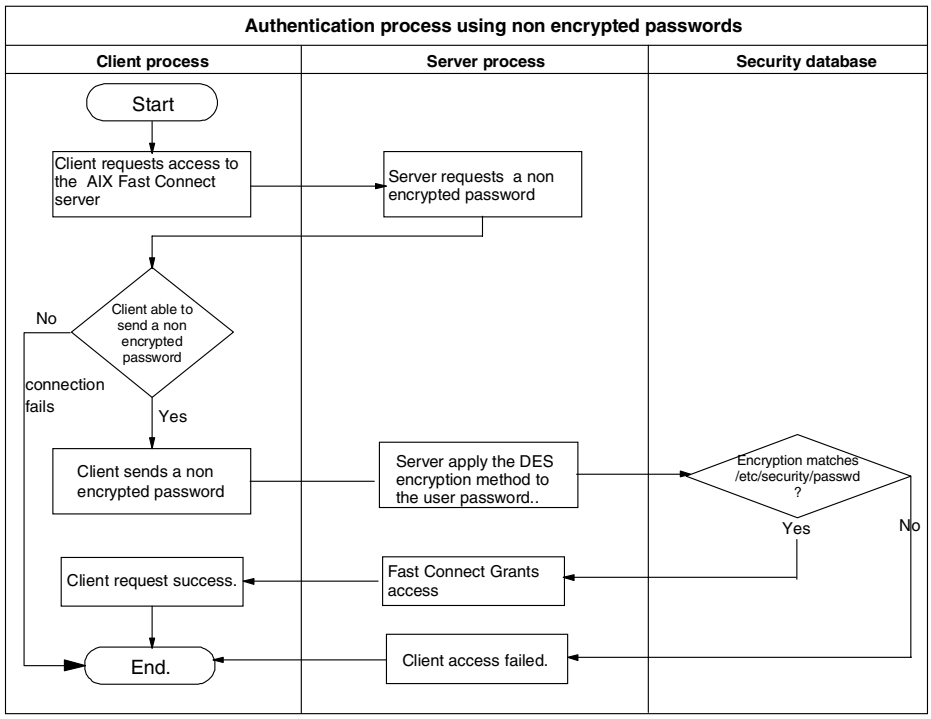


Figure 65. Authentication process using non-encrypted passwords

There are several ways to customize the server to use non-encrypted passwords.

9.1.1 Using WebSM

The following is the procedure to configure AIX Fast Connect server to use non-encrypted passwords from WebSM.

1. Select the **PC services** icon; a list appears with the AIX Fast Connect server and the shared resources. See Figure 66 on page 93.

Figure 66. The WebSM interface using Internet browser

2. Select the AIX Fast Connect server name and right-click the **Properties** option. The properties page for the AIX Fast Connect server appears as shown in Figure 67 on page 94 and Figure 68 on page 95.

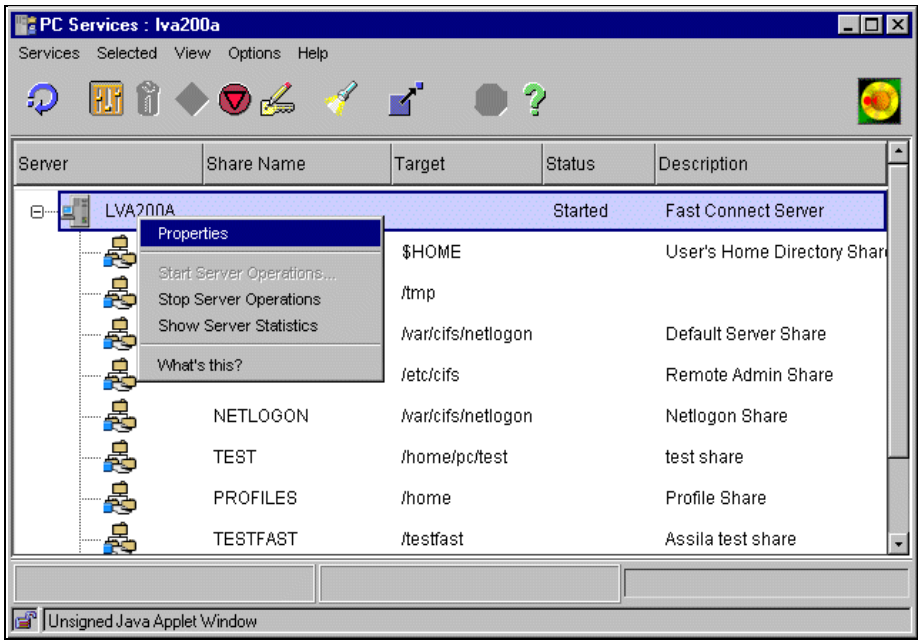


Figure 67. AIX Fast Connect connect administration interface from WebSM

3. Select the **Network Access** tab and uncheck the **Use encrypted passwords** option as shown in Figure 68 on page 95.

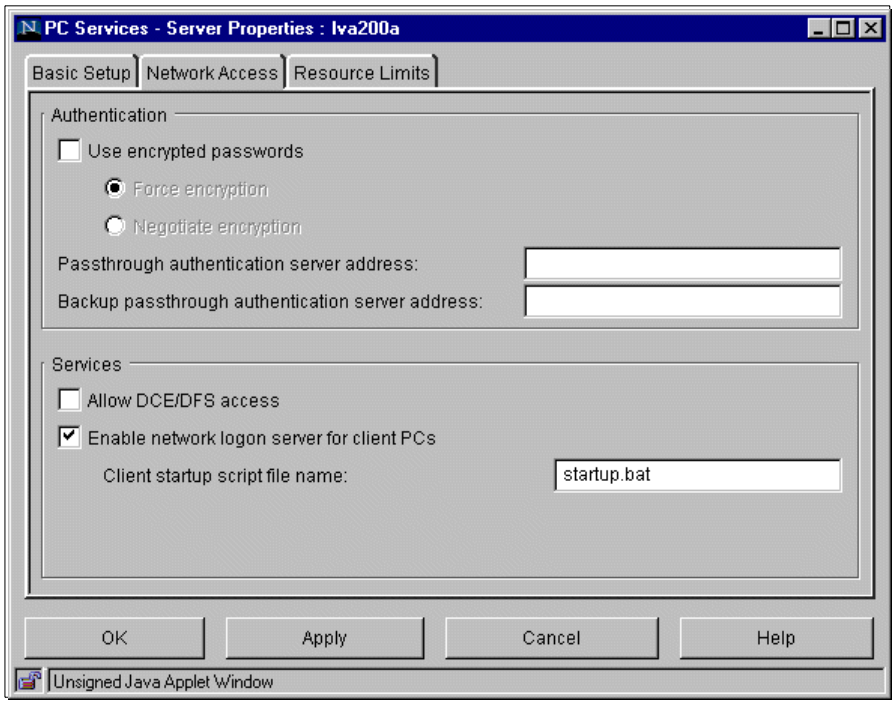


Figure 68. Properties option of AIX Fast Connect server

4. Press the **OK** button.
5. Stop and restart AIX Fast Connect services.

9.1.2 Using SMIT

Perform the following steps to configure AIX Fast Connect to use the non-encrypted passwords option using SMIT.

Enter the following command at the system prompt to start SMIT with the fastpath option:

```
smitty smbcfghatt
```

6. Set the Use Encrypted Passwords option to **no**, and press the **Enter** key as shown in Figure 69 on page 96.

```
                                Attributes

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

[TOP]                                                  [Entry Fields]
* Server Name                                         [lva200b]
* Start Server                                        [Now]                    +
* Domain Name                                         [LVA200]
  Description                                         [ Fast Connect Server]
  Server alias(es)
  WINS Address                                        [9.3.240.230]
  Backup WINS address                                 [ ]
  Proxy WINS Server                                   [off]                    +
  NetBIOS Name Server (NBNS)                          [off]                    +
  Use Encrypted Passwords                             [no]                     +
  Passthrough Authentication Server                   [ ]
  Backup Passthrough Authentication Server            [ ]
  Allow DCE/DFS access                                [no]                     +
[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
```

Figure 69. SMIT AIX Fast Connect server properties interface

7. Stop and restart AIX Fast Connect services.

9.1.3 Modifying the clients to send non-encrypted passwords

In some cases, it is necessary to set up the clients to send encrypted or non-encrypted passwords. Table 1 describes the default configuration for common clients.

Table 1. Default encryption mechanisms for Windows operating systems

Operating system	Can send non-encrypted passwords by default	Comments
Windows 95 with vredir.vxd earlier than 4.00.1114 and vnetsup.vxd earlier 4.00.1112.	Yes	***Vrdupd.exe*** updated file is required and changes on the registry database to solve this security issue.
Windows 95 vredir.vxd version 4.00.1114 or later and vnetsup.vxd 4.00.1112 or later.	No	Changes on the registry database are required.

Operating system	Can send non-encrypted passwords by default	Comments
Windows 98	No	Changes on the registry database are required.
Windows NT 4.0 and SP < 3	Yes	Service pack 3 or newer required to solve this security issue.
Windows NT 4 and SP ≥ 3	No	Changes on the registry database are required
Windows 2000	No	Changes on security police profile are required.

9.1.3.1 Windows 95

The latest versions of Windows 95 only send encrypted passwords through the network. To check the version of your environment, look at the level of these two files:

- vredir.vxd Version 4.00.1114 or later
- vnetsup.vxd Version 4.00.1112 or later

These updates come in the ***vrdupd.exe*** file update and can be obtained from the Microsoft Web site at the following URL:

```
http://support.microsoft.com/download/support/mslfiles/vrdrupd.exe
```

It is also required to check whether the following registry entry exists and that the value of this entry is set to the correct value, or else, it is necessary to create the registry entry and restart the machine:

```
Registry key:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\VNETSUP
Type registry entry: Dword
Registry entry: EnablePlainTextPassword = 1
(1 = Send non encrypted passwords, 0 = Only send encrypted passwords)
```

9.1.3.2 Windows 98 and Windows 98 SE

The Windows 98 versions always had the default of sending encrypted passwords through the network. However, in some configurations, it might be necessary to set up the Windows 98 clients to send non-encrypted passwords. In the Windows 98 versions, it is necessary to modify the registry database on the same registry key and entry as Windows 95. The Windows 98 versions have two ways of performing this task:

- If you do not have the Windows 98 SE CDROM, it is necessary to check whether the following registry entry and the value exist, or else, it is necessary to modify the registry entry and restart the machine:

  ```
  Registry key:
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\VNETSUP
  Type registry entry: Dword
  Registry entry: EnablePlainTextPassword = 1
  ```

- If you have the Windows 98 SE CDROM, select the **PTXT_ON.INF** file from the \tools\mtsutil directory, right-click, select the **install** option to create the following registry entry, set it to 1, and restart the machine.

  ```
  Registry key:
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\VNETSUP
  Registry entry: EnablePlainTextPassword = 1
  ```

9.1.3.3 Windows NT 4.0 and Service Pack before V3

In Windows NT 4.0 with Service Pack earlier than Version 3, it is not necessary to do anything because these versions use both methods (encrypted and non-encrypted) by default. This is a security risk and is fixed with service pack 3 or later.

9.1.3.4 Windows NT 4.0 and SP 3 or later

Windows NT 4.0 with service pack 3 or later only send encrypted passwords by default, and it is necessary to change the registry to allow Windows NT 4.0 clients to send non-encrypted passwords if the authentication with encrypted passwords fails. You will have to modify the registry as described in the following and restart the machine:

```
Registry key:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rdr\Parameters
Type registry entry: Dword
Registry entry: EnablePlainTextPassword = 1
(1 = Send non encrypted passwords, 0 = Only send encrypted passwords)
```

9.1.3.5 Windows 2000

The different versions of Windows 2000 send encrypted passwords by default, and it is necessary to make changes to the security policy profile to allow Windows 2000 to send non-encrypted passwords if the authentication with encrypted passwords fail. The required changes are described in the following steps:

1. Select the **Administrative tools** group from the Start menu programs or the Control panel, and double-click.
2. Select the **Security policy** icon, and double-click.

3. Select the **Local policies** subtree and double-click.
4. Set the **Send unencrypted password to connect to third_party SMB servers** option to **enable**.
5. Restart the machine.

9.2 Using AIX Fast Connect with encrypted passwords

We have seen that the default configuration for Fast Connect was to expect clear text passwords. It is necessary to set up a parameter to accept encrypted passwords and increase the network security, thus preventing the server from accepting non-encrypted passwords from the clients.

When the encrypted option is enabled, it is necessary to pay attention to the AIX Fast Connect server users because, when this option is enabled, an additional user and password database using the RSA encryption method used by Windows clients is required. This database is located in the /etc/cifs/cifsPasswd file.

The flow chart, shown in Figure 70, illustrates the authentication process when the encryption option is enabled.

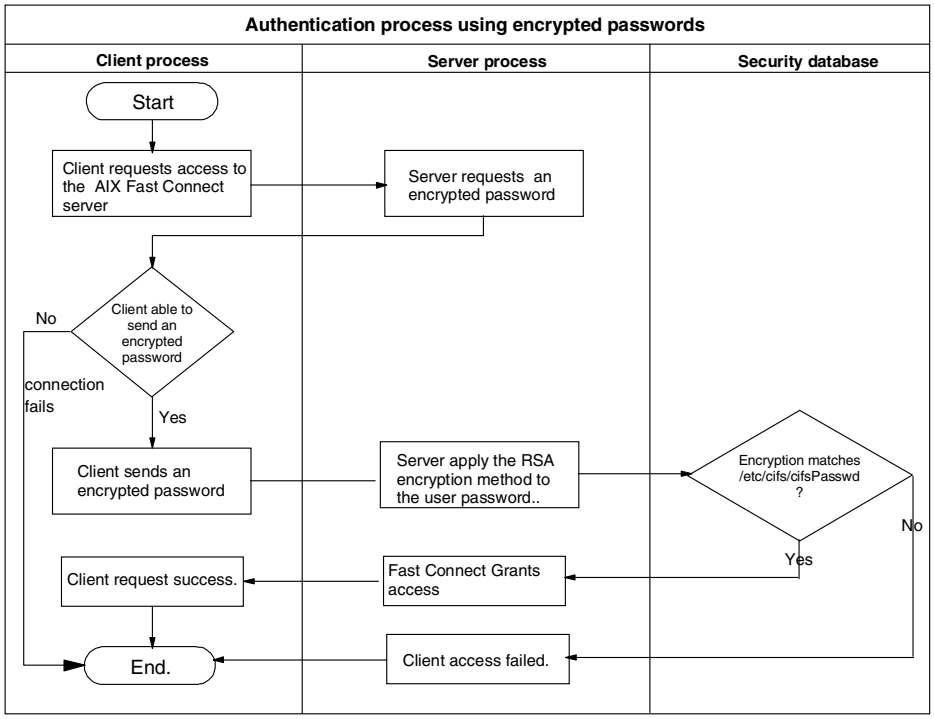


Figure 70. Authentication process using encrypted passwords

There are different ways to customize the server to accept only encrypted passwords from clients.

9.2.1 Using WebSM to customize AIX Fast Connect server

The following is the procedure to configure AIX Fast Connect server, with the WebSM tool, to only use encrypted passwords:

1. Select the **PC services** icon and double-click; a list with the AIX Fast Connect server and the shared resources appears as shown in Figure 71 on page 101.

Figure 71. WebSM interface using Internet browser

2. Select the AIX Fast Connect server name and right-click to choose the **Properties** option. The properties page for the AIX Fast Connect server appears as shown in Figure 72 and Figure 73 on page 102.

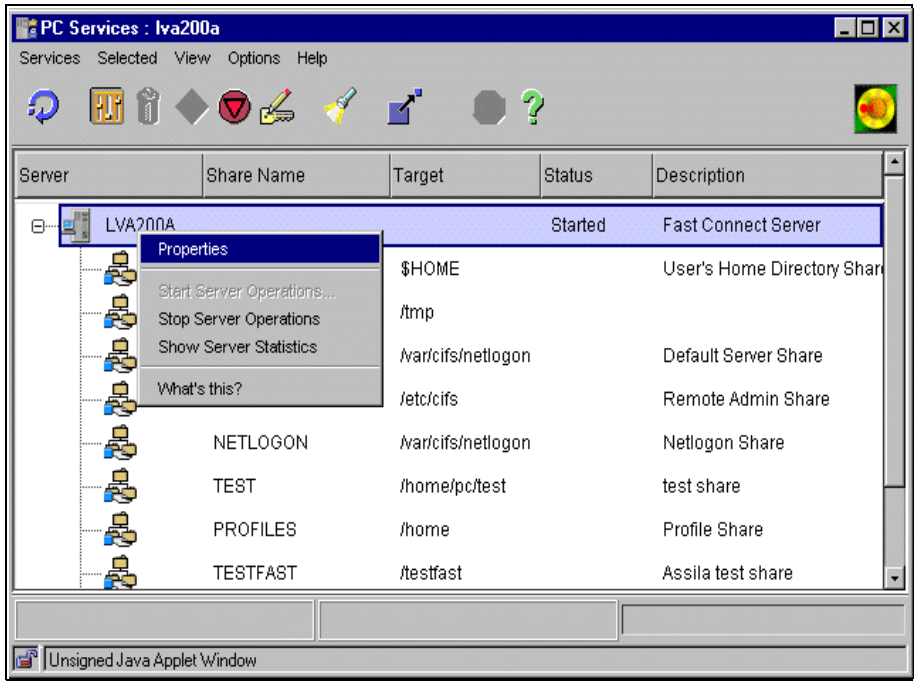


Figure 72. AIX Fast Connect administration interface from WebSM

3. Select the **Network Access** tab, check the **Use encrypted passwords** option, and verify that the **Force encryption** radio button option is also selected. See Figure 73.

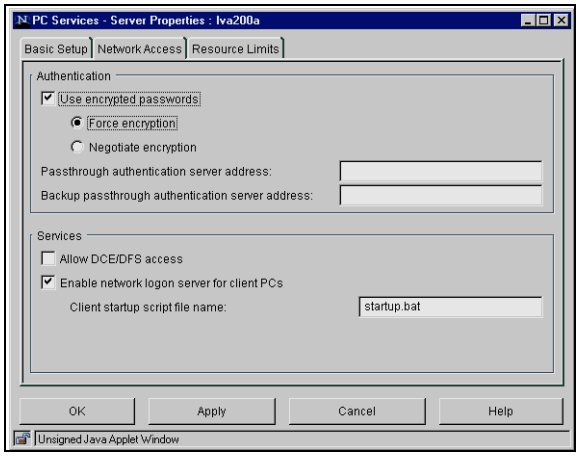


Figure 73. Properties option of AIX Fast Connect server

4. Press the **OK** button.
5. Stop and restart AIX Fast Connect services.

9.2.2 Using SMIT

Follow the next steps to configure AIX Fast Connect to use the encrypted passwords option using the SMIT administration tool:

1. Enter the following command at the system prompt to start SMIT with the fastpath option:

   ```
   smitty smbcfghatt
   ```

The SMIT AIX Fast Connect server properties interface is shown in Figure 74.

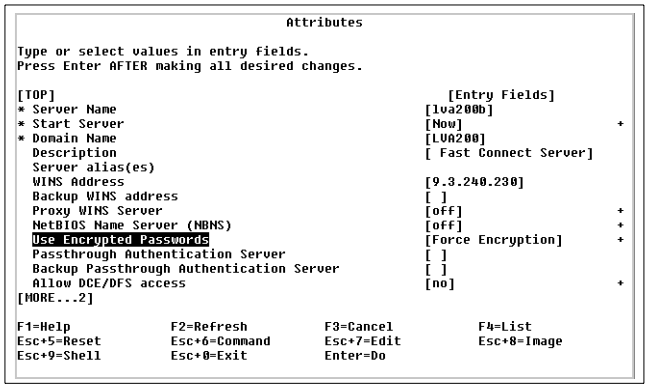


Figure 74. SMIT AIX Fast Connect server properties interface

2. Set the **Use Encrypted Passwords** option to **Force Encryption**, and press the **Enter** key. See Figure 74.
3. Stop and restart AIX Fast Connect services.

9.2.3 Creating AIX Fast Connect users

As mentioned previously, it is required to administer a second user database where the user and passwords will be stored using the Windows-specific encryption method. You can use the WebSM interface, SMIT tool or command line options to create AIX Fast Connect users.

9.2.3.1 Using WebSM to create AIX Fast Connect users

To create AIX Fast Connect users using the WebSM interface, perform the following steps:

1. Start the **PC services** icon located on the main window of the WebSM administration tool.
2. Select the **AIX Fast Connect server**.
3. Select the **User Administration** option located in the Services submenu; the Fast Connect User Administration window appears as shown in Figure 75.

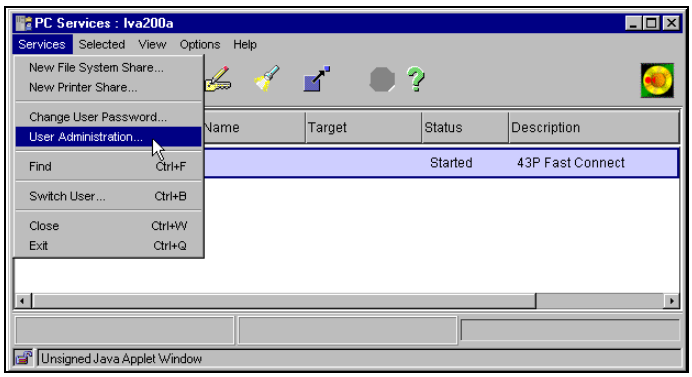


Figure 75. PC services console

4. Click the **Create User** button, and fill the information required to create the user. See Figure 76.

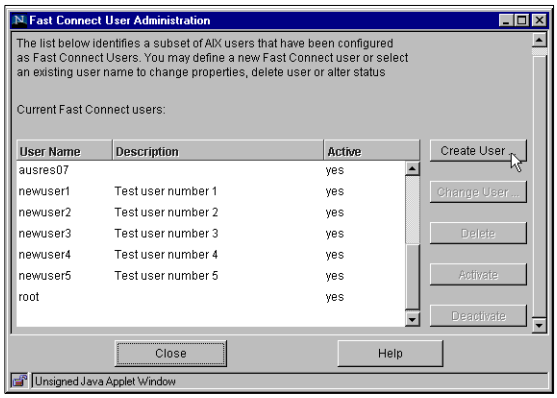


Figure 76. Fast Connect User Administration

5. Input the following fields required to create an AIX Fast Connect user. See Figure 77 on page 105.

- **User Name**: Specify an existing AIX user name, this user name will be created in the AIX Fast Connect users database.
- **Password**: Specify the password for this user, this password will be encrypted using the Windows method and stored in the ***/etc/cifs/cifsPasswd*** file.
- **Confirm password**: Specify the password again, this is for confirmation.
- **Description**: Optional field, used to provide a brief description of this AIX Fast Connect users.
- **Activate user account**: This is a check box field; check this box to automatically activate the user account on the AIX Fast Connect server.

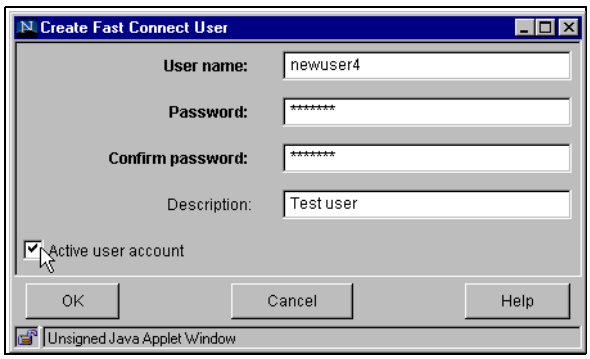


Figure 77. Create Fast Connect User

6. Press the **OK** button to create the user.

9.2.3.2 Using SMIT to create AIX Fast Connect users

Perform the following steps to create AIX Fast Connect users using SMIT:

1. Enter the following command at the system prompt to start SMIT:

```
smitty smbcfgusradd
```

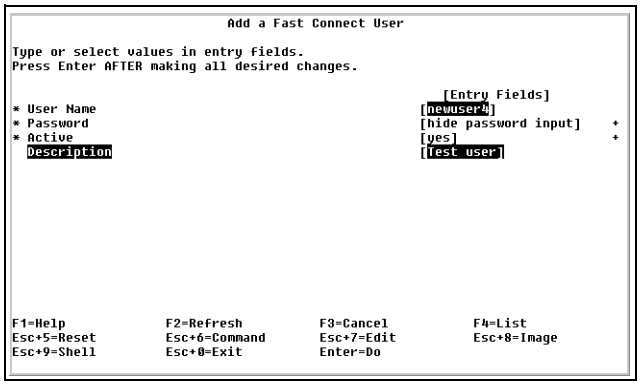


Figure 78. Add a Fast Connect User

2. Input the following fields required to create an AIX Fast Connect user. See Figure 78:
   - **User Name**: Specify an existing AIX user name. This user name will be created in AIX Fast Connect users database.
   - **Password**: Select **hide password input** or **show password input** to show or hide the password during the user creation process. Remember that this password will be encrypted using the Windows method and stored in the /etc/cifs/cifsPasswd file.
   - **Active**: Specify whether the use account will be automatically activated on the AIX Fast Connect server.
   - **Description**: Optional field used to provide a brief description of AIX Fast Connect users.
3. Press the **Enter** key and enter the user password; the user is created.

9.2.3.3 Creating AIX Fast Connect users from the command line

From the command line, issue the following to create AIX Fast Connect users:

```
# net user sales demo01 /add /active:yes /comment:"User of sales team"
# Command completed successfully.
# net user
User Name                      User Comment
----------                     ------------
root                           System administrator
newuser1                       Test user
sales                          User of sales team
ausred08                       Residencie user
#
```

This command creates a user with these characteristics:

- **Username**: sales
- **Password**: demo01
- **Activate**: Yes
- **Description**: User of sales team.

9.2.4 Changing AIX Fast Connect passwords

When the encryption method is enabled on the AIX Fast Connect server, it is necessary to manage the AIX Fast Connect users and one of the tasks is to change the users' passwords. We will describe different methods of changing the AIX Fast Connect users' passwords using the WebSM interface, the SMIT interface, and the command line interface.

9.2.4.1 Using WebSM

To change the AIX Fast Connect user password using the WebSM interface, perform the following steps:

1. Start the ***PC services*** icon located on the main window of the WebSM administration tool.
2. Select the AIX Fast Connect server.
3. Select the **User Administration** option located in the Services submenu. The Fast Connect User Administration window, shown in Figure 79 on page 107, will appear.

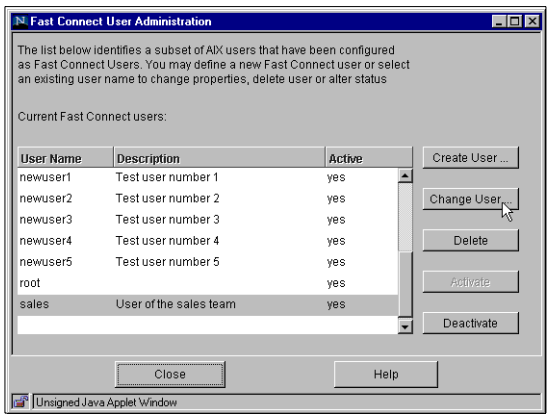


Figure 79. Fast Connect User Administration

4. Select the user and the **Change User** button. The Fast Connect user properties windows appears as shown in Figure 80.

Figure 80. Fast Connect User Properties

5. Enter the new password and confirm the password. See Figure 80.
6. Press the **OK** button to change the password.

9.2.4.2 Using smit

Perform the following steps to change AIX Fast Connect user passwords using SMIT:

1. Enter the following command at the system prompt to start SMIT, and select the **Change a User's Password** option:

   ```
   smitty smbcfgusr
   ```

2. Select the user who needs a password change. See Figure 81 on page 108.

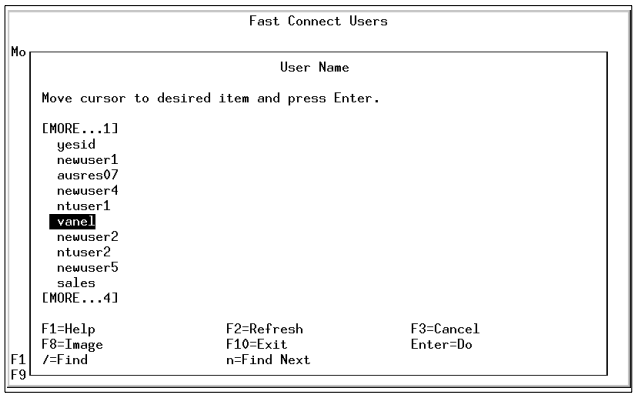


Figure 81. Fast Connect Users

3. Enter this new user's password. See Figure 82.

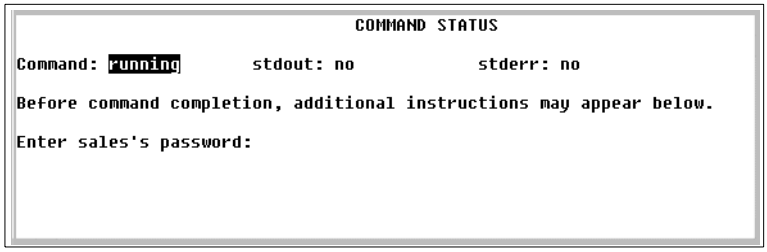


Figure 82. Changing AIX Fast Connect user's password window from SMIT

4. Press the **Enter** key. The user's password has been changed.

9.2.4.3 Using the command line

You can also use the command line to change AIX Fast Connect user passwords.

The following examples show the command to change the user password:

- **Username**: sales
- **New password**: demo

```
# net user sales -p
Enter sales's password:
Command completed successfully.
#
```

Or enter the user's password directly in the command line:

```
# net user sales demo
Command completed successfully.
#
```

9.2.5 Synchronizing AIX Fast Connect and AIX passwords

When the encrypted password option is enabled, it is necessary to manage two user's password databases. The first one is located in the /etc/security/passwd file; these are the AIX user passwords. The second one is located in the ***/etc/cifs/cifsPasswd*** file; this one is used by the AIX Fast Connect server on the authentication process when the encryption option is enabled.

9.2.5.1 Using WebSM to synchronize passwords

To synchronize the AIX Fast Connect and AIX user passwords using the WebSM interface, perform the following steps:

1. Start the **PC services** icon located on the main window of the WebSM administration tool.
2. Select the AIX Fast Connect server.
3. Select the **Change User Password** option located in the Services submenu shown in Figure 83.

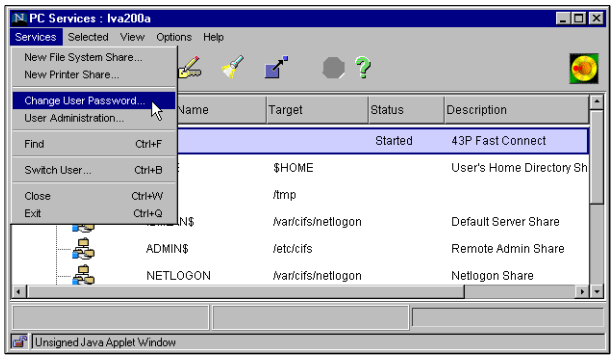


Figure 83. AIX Fast Connect server administration window

4. In the Change user password window, enter the new password and confirm the password. For both databases to be synchronized, the **Change AIX password to match the one entered above** option must be checked as shown in Figure 84.

Figure 84. Change User Password

5. Press the **OK** button to change and synchronize the passwords.

9.2.5.2 Synchronizing passwords with the command line

To synchronize passwords from the command line, you have to add the /changeaixpwd:yes option to the usual command for changing the AIX Fast Connect passwords explained in Section 9.2.4.3, “Using the command line” on page 109.

```
# net user sales -p /changeaixpwd:yes
sales's New password:
Enter the new password again:
Command completed successfully.
#
```

Or, enter the user password directly in the command line:

```
# net user sales demo01user /changeaixpwd:yes
Command completed successfully.
#
```

9.3 Using AIX Fast Connect in a mixed environment

In some cases, it is necessary to enable this option to accept clients that only support non-encrypted passwords and other clients with encrypted passwords.

9.3.1 Using WebSM to customize AIX Fast Connect server

To configure AIX Fast Connect server to accept encrypted and non-encrypted password using the WebSM administration tool, perform the following steps:

1. Select the **Network Access** tab from the Server Properties option on **PC Services -> Services -> Properties -> Network Access**. See Figure 85.

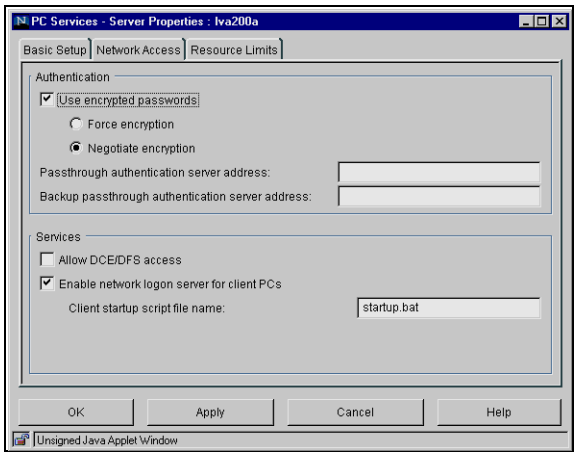


Figure 85. Server Properties window using WebSM

2. Select the **Use encrypted passwords** option and verify that the **Negotiate encryption** radio button option is also selected. See Figure 85.
3. Click the **OK** button.
4. Stop and restart AIX Fast Connect services.

9.3.2 Using SMIT

Perform the following steps to configure AIX Fast Connect to use encrypted and non-encrypted passwords option using SMIT:

1. Enter the `smitty smbcfghatt` command at the system prompt to start SMIT. See Figure 86 on page 112.

```
                                Attributes

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

[TOP]                                                   [Entry Fields]
* Server Name                                          [lva200b]
* Start Server                                         [Now]                    +
* Domain Name                                          [LVA200]
  Description                                          [ Fast Connect Server]
  Server alias(es)
  WINS Address                                         [9.3.240.230]
  Backup WINS address                                  [ ]
  Proxy WINS Server                                    [off]                    +
  NetBIOS Name Server (NBNS)                           [off]                    +
  Use Encrypted Passwords                              [Negotiate Encryption]   +
  Passthrough Authentication Server                    [ ]
  Backup Passthrough Authentication Server             [ ]
  Allow DCE/DFS access                                 [no]                     +
[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
```

Figure 86. SMIT AIX Fast Connect server properties interface

2. Set the Use Encrypted Passwords option to **Negotiate Encryption**, and press the **Enter** key as shown in Figure 86.
3. Stop and restart AIX Fast Connect services.

9.4 AIX Fast Connect server with Passthrough authentication

The passthrough authentication option enables the AIX Fast Connect server to accept clients that have been validated by a Primary Domain Controller or Backup Domain Controller servers on the network. This is an administrative advantage because it is not necessary to manage two databases of users on AIX, and you do not need to manage the AIX Fast Connect server users anymore. However, it requires you to have a corresponding AIX user (only passwords do not need be managed) for every user validated from the PDC or BDC server.

Using this option, you have a two-level process; the first one is using a PDC or BDC server to try and validate the users passwords. If PDC or BDC from the network cannot authenticate the user, the AIX Fast Connect server then tries to authenticate the users with the local database using the different options explained previously.

The flow chart, shown in Figure 87 on page 114, illustrates the authentication process when the passthrough option is used.

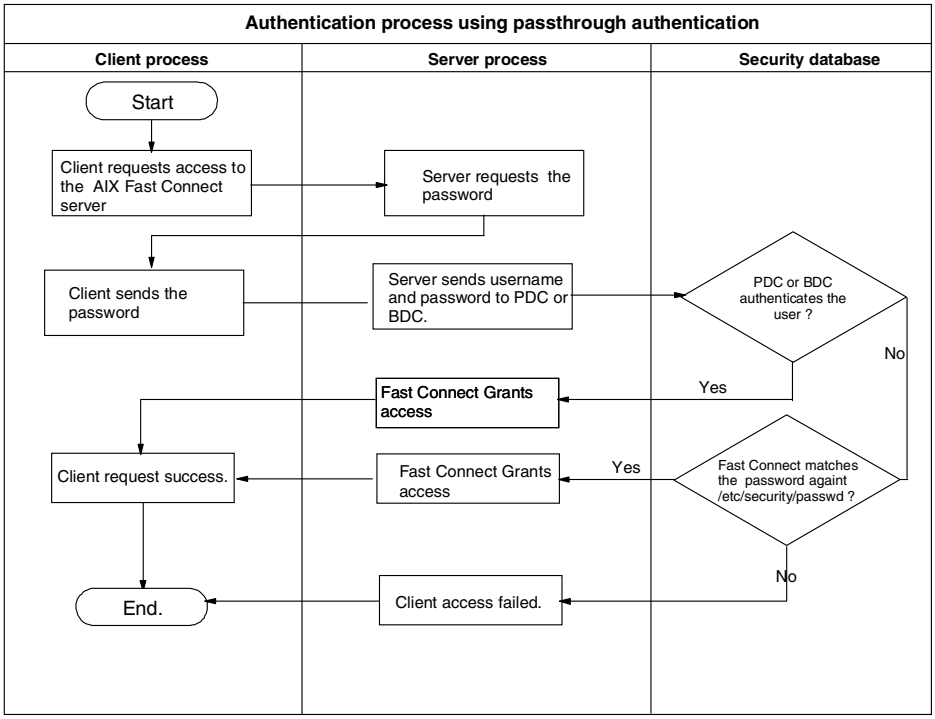


Figure 87. Authentication process using passthrough authentication

There are different ways to customize the Fast Connect server to use the Passthrough option to authenticate clients.

9.4.1 Using WebSM to customize AIX Fast Connect server

To configure AIX Fast Connect server to use the Passthrough authentication option using the WebSM administration tool, perform the following steps:

1. Select **Network Access** from the Server Properties option on: ***PC Services -> Services -> Properties -> Network Access***. See Figure 88 on page 115.

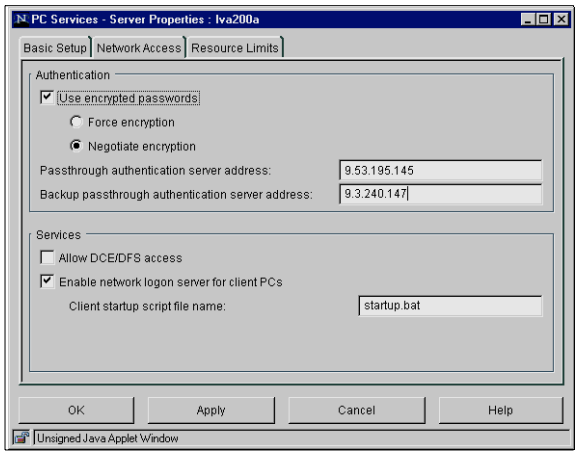


Figure 88. Server Properties window using WebSM

2. Enter the NetBIOS name or IP address of the PDC server on the Passthrough authentication server address field, and enter the NetBIOS name or IP address of the BDC server in the Backup passthrough authentication server address field.
3. Push the **OK** button.
4. Stop and restart AIX Fast Connect services.

9.4.2 Using SMIT

Perform the following steps to configure AIX Fast Connect to use the Passthrough authentication option using SMIT:

1. Enter the following command:

   ```
   smitty smbcfghatt
   ```

2. Enter the NetBIOS name or IP address of the PDC server on the Passthrough authentication server address field and the NetBIOS name or IP address of the BDC server on the Backup passthrough authentication server address field as shown in Figure 89 on page 116.

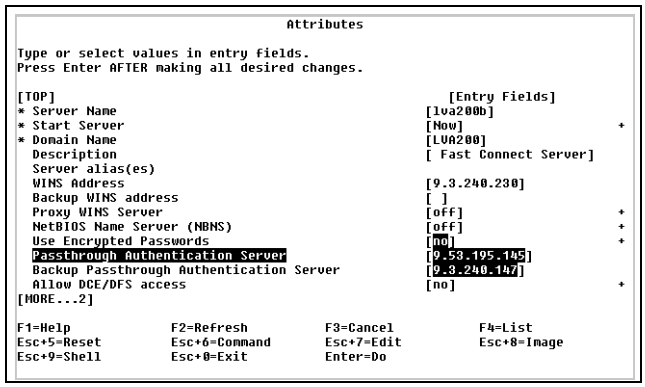


Figure 89. SMIT AIX Fast Connect server properties interface

3. Stop and restart AIX Fast Connect services.

Chapter 10. Using Netlogon

The Netlogon feature was integrated with the Fast Connect product starting with Version 2.1.1. This allows centralized management of the user profiles and system policies. The Fast Connect product does not support other Domain Controller functions.

Netlogon support in the Fast Connect server is composed of two features: User profiles and System policy. A user profile is a configuration for a specific user, which covers the user's environment and preference settings, such as desktop icons, color options, and installed applications. System policy defines the computer resources that can be enabled/disabled by a system administrator. System policy can be assigned to users or groups of users.

10.1 Configuration of the Fast Connect server

You can define four options with which to modify the location of the Netlogon files on the Fast Connect server:

- **networklogon** - Enables or disables netlogon support.
- **startup_script** - Specifies a startup script to use during the logon. The default value is startup.bat. You can use two meta tags to specify computer name (%U) or user name (%N).
- **profiles_path** - Specifies a path to the PROFILES share. The default value is /home. Profile data is stored in this directory (in the user's home directory).
- **netlogon_path** - Specifies a path to the NETLOGON share. The default value is /etc/cifs/netlogon. Startup scripts and policy files are stored in this directory.

You can start the Netlogon support from a Web-based System Manager (WebSM), SMIT, or with the `net` command. The first two can be used only if you just want to enable/disable netlogon support or set the startup script name. The last one (the `net` command) is used to set all four parameters. You must restart the Fast Connect server after these changes.

If you are using WebSM, then you must open the **System Properties** window from the main Fast Connect window. You can do this by selecting the Fast Connect server line and then clicking **Selected** / **Properties** as shown in Figure 90 on page 118.

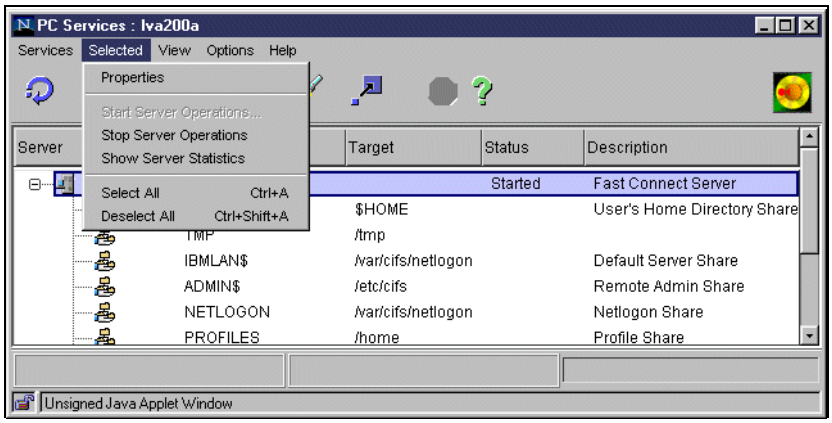


Figure 90. Fast Connect server properties selection in WebSM

After that you will see the window, shown in Figure 91, where you can enable/disable netlogon support.

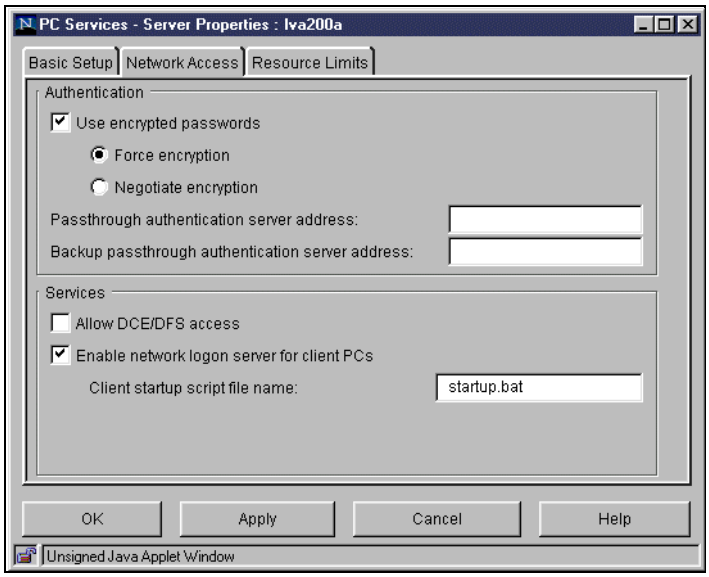


Figure 91. Selecting netlogon in the Fast Connect properties window

If you use the `smit` command, you can use the smbcfghatt fastpath.

You can set all four parameters for the netlogon support with the `net` command with the following syntax:

```
net config [ options ]
```

You can use the following options:

- **/networklogon:0|1** - Disables/enables the netlogon support
- **/startup_script:script** - Specifies a startup script name.
- **/profiles_path:path** - Specifies a path to the PROFILE share.
- **/netlogon_path:path** - Specifies a path to the NETLOGON share.

The following is a example of a simple start of the netlogon support from the command line:

```
# net config /netlogon:1
Command completed successfully.
```

10.1.1 Preparing the profile scripts

The profile scripts are DOS batch files that are executed on the client computer automatically at the logon of the client. The location and the name of these scripts depend on the client type and the logon method used. They must be valid DOS files; so, you must add an '^M' character (carriage return) at the end of the line if you are editing them from the AIX. Here is one example of such a script that performs mapping of a computer share:

```
@echo off^M
net use h: \\lva200a\home^M
echo "H: is now mapped to \\lva200a\home^M
~
~
~
"startup.bat" 3 lines, 95 characters
```

You can use the pause command in the profile script if you want to stop the execution of the script at one point.

10.1.2 Configuring the system policy

When you are creating the system policy for a mixed environment with Windows NT and Windows 95/98 clients, you must create two different configurations, one for each client type.

System Policy is located in a NETLOGON share. You must use a System Policy Editor to change the policy settings. Settings must be saved in a NETLOGON share. The file name for the Windows NT system policy is

NTconfig.pol, and, for the Windows 95/98 system policy, it is config.pol. The owner of the system policy file on the Fast Connect server should be a non-root user.

10.1.2.1 Configuration from the Windows NT client

You can run the Policy Editor with **Start -> Programs -> Administrative Tools (Common) -> System Policy Editor**. System policy must be saved on the Fast Connect machine under the name NTconfig.pol.

10.1.2.2 Configuration from the Windows 95/98 client

By default, Windows 95 does not have the system policy editor installed. You must install it from the Upgrade or Retail CD, or you can install it from the Windows NT Server v4.0:

Installation from the Windows 95 CD:

1. Open the Control Panel and select **Add/Remove Programs**.
2. Click on the **Windows Setup** tab and select **Have Disk**.
3. Select the \Admin\Apptools\Poledit\ directory on CD.
4. Install **Group Policies** and **System Policy Editor**.
5. Now, you can run the Policy Editor with **Start -> Run -> poledit**.

installation from the Windows NT v4.0 server:

1. Copy Poledit.exe from the base Windows directory on the Windows NT server (\winnt) to the base Windows directory on the Windows 95 client (\windows)
2. copy Common.adm and Windows.adm from the subdirectory of the base Windows directory on the Windows NT server (\winnt\inf) to the equivalent directory on the Windows 95 client (\windows\inf).
3. Now, you can run the Policy Editor with **Start -> Programs -> Accessories -> System Tools -> System Policy Editor**.

The system policy file for Windows 95/98 clients must be saved on the Fast Connect server in the NETLOGON share with the name config.pol. When you create a new policy file, save it on the local computer and transfer it manually to the Fast Connect server. Then, you can change the ownership of the file to the responsible (not necessarily root) user.

You can open/change/save an existing config.pol file directly from the System Policy editor.

10.1.3 Configuring NT clients from a different subnetwork

You can configure the Windows NT clients from a different subnetwork to use the netlogon function of the Fast Connect server. You must use encrypted passwords between these clients and the server. The Fast Connect server must use a different domain name than the domain controller used by these clients.

Note

Make sure that you have only one AIX Fast Connect server and no domain controllers with the netlogon support enabled on the subnetwork.

If the client is not on the same subnetwork as the logon server, you will need to make some modifications to the name resolution in LmHOSTS file or on the NetBIOS Name Server. You must add an entry that will map *domain name* with the subcodes, <00> and <1C>, to the Fast Connect server. Here is an example of an LMHOST file entry for the Fast Connect server at the IP address 9.3.240.215:

```
9.3.240.250   lva200                  #PRE #DOM:lva200
9.3.240.250   "lva200        \0x00"    #PRE
9.3.240.250   "lva200        \0x1C"    #PRE
```

`#PRE` indicates that the entry must be preloaded and `#DOM` maps the server to the specified domain name.

You will also need at least one master browser with the same workgroup name as the Fast Connect server.

10.2 Configuring the IBM Network Client

Before using the Netlogon, users on the clients must also be configured. Windows NT can only work with the Fast Connect server if they have installed IBM Network Client; so, if you have Windows NT and Windows 95/98 in the network, you should probably use the IBM Network Client for all the clients.

10.2.1 Configuring IBM Network Client on the Windows NT client

The netlogon support on the Windows NT requires encrypted passwords and the IBM Network client. You can download the IBM Network client from the following Web site:

`http://service.boulder.ibm.com/asd-bin/doc/en_us/winntcl2/f-feat.htm`

After you extract the archive to a directory, run **Start -> Settings -> Control Panel -> Network** and select **Services**. See Figure 92.

Select the **Identification** tab and set the workgroup (not the domain!) to the name of the Fast Connect server workgroup name.

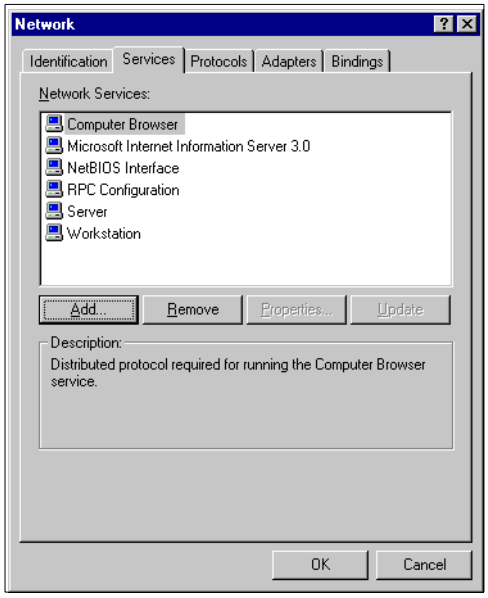


Figure 92. Adding new network service in Windows NT

Then, press the **Add** button, and, in a Select Network Service window, press the **Have disk** button. In the Insert disk dialog window, enter the full path to the directory with the extracted archive and press **OK**. You will see the Select OEM Option window shown in Figure 93; select **IBM Networks Primary Logon Client for Windows NT**.

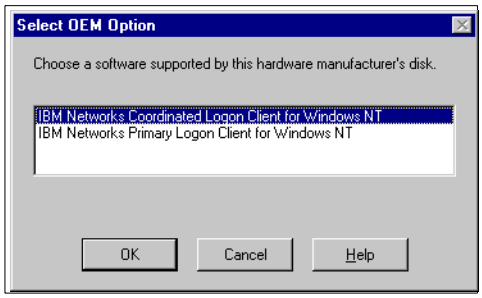


Figure 93. Select OEM Option

From the screen shown in Figure 94, enter the Fast Connect server domain name in the Domain name field and press the **OK** button.

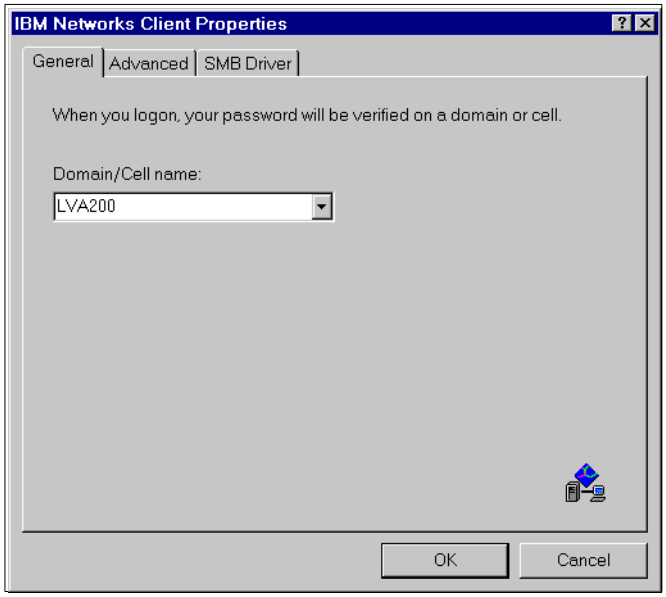


Figure 94. General properties of IBM Network Client for NT

10.2.2 Configuring IBM Network Client on the Windows 95/98 client

You can use the IBM Network Client or Microsoft Client on Windows 95/98 clients. IBM Network client is available from the following Web site:

`http://service.boulder.ibm.com/asd-bin/doc/en_us/win95cl2/f-feat.htm`

After you extract the archive to a directory, run **Start -> Settings -> Control Panel -> Network** (see Figure 99 on page 127).

Select the **Identification** tab and set the workgroup to the name of the Fast Connect server workgroup name.

Select the **Configuration** tab and then press the **Add** button. Select **Client** type in the Select Network Component Type windows, and press the **Add** button. In the Select Network Client window, shown in Figure 96 on page 124, press the **Have disk** button.

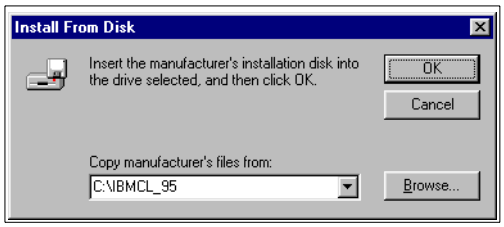


Figure 95. Location of the IBM Network Client for Windows 95 distribution

In the Install From Disk dialog window, enter a full path to the directory with the extracted archive and press **OK**.

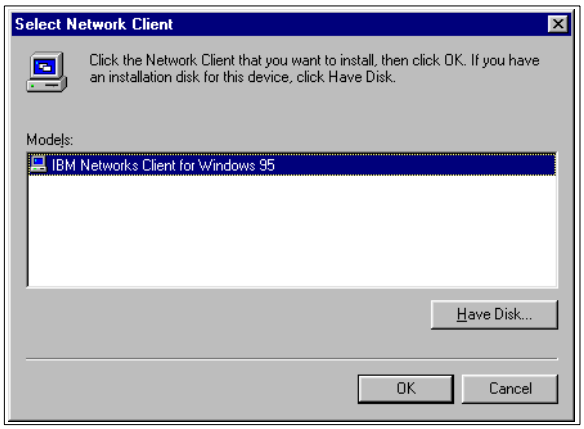


Figure 96. Select Network Client

You will see a Select Network Client window. Confirm the only option by pressing the **OK** button, and the IBM Network Client will be installed. In a Network window (see Figure 99 on page 127), select **IBM Network Client for Windows 95** and press the **Properties** button.

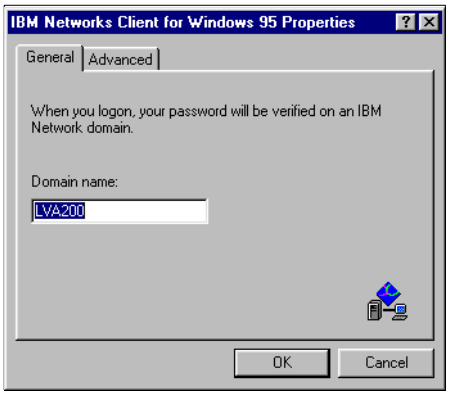


Figure 97. IBM Network Client properties

Enter the name of the domain as defined in the Fast Connect server.

If you also want to enable System Policy download from the Fast Connect server, you must make one additional change in the Advanced tab as shown in Figure 98.

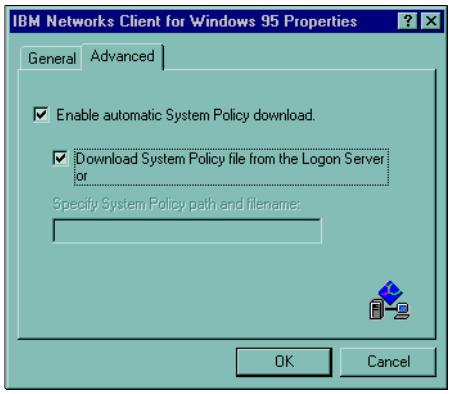


Figure 98. IBM Network Client advanced properties

Check the Enable automatic System Policy download box and the Download System Policy file from the Logon Server box.

Then, press the **OK** button to confirm the changes. Change the Primary Network Logon entry in the Network configuration window (see Figure 99 on page 127) to IBM Network Logon. You must reboot the computer after the installation and customization.

10.2.3 Using the IBM Network Client

After installation and configuration of the IBM Network Client, you should configure the profile scripts to meet your requirements. They can be executed from two different sources:

- The profile.bat script in the HOME share.
- The startup script, located in the NETLOGON share. Its name is defined in the Fast Connect server. It can be a global, per-user, or per-computer startup script (see the startup_script parameter in Section 10.1, “Configuration of the Fast Connect server” on page 117).

You can specify both scripts, and they will both be executed at user logon. The user profile is saved on the Fast Connect server in the HOME share. Windows 95/98 saves it in the root directory, and Windows NT saves it in the Profiles subdirectory.

10.3 Configuring the Microsoft Network Client

You can use the Fast Connect netlogon support on Windows 95/98 client without any additional configuration. Microsoft Network Client offers fewer possibilities than the IBM Network Client and does not allow connection of the Windows NT clients to the Fast Connect server. If you only have Windows 95/98 on the network and do not require any of the special features provided by IBM Network Client, you can use Microsoft Network Client.

You can enable Microsoft Network Client support with **Start -> Settings -> Control Panel -> Network**. See Figure 99 on page 127.

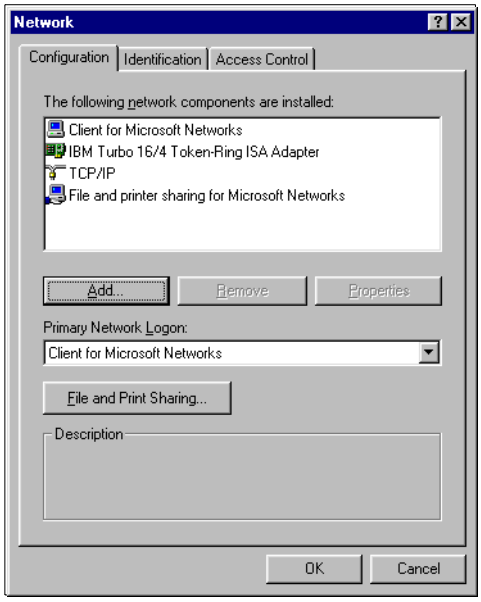


Figure 99. Network configuration window in Windows 95

If you do not see the Client for Microsoft Networks component in the list, you must install it. Press the **Add** button. Select the **Client** entry in the list and press the **Add** button. Select the **Microsoft** entry from the list of manufacturers and select **Client for Microsoft Network** from the list of network clients. Press the **OK** button to install the client.

Double-click on the **Client for Microsoft Networks** to change its properties. The screen, shown in Figure 100 on page 128, appears.

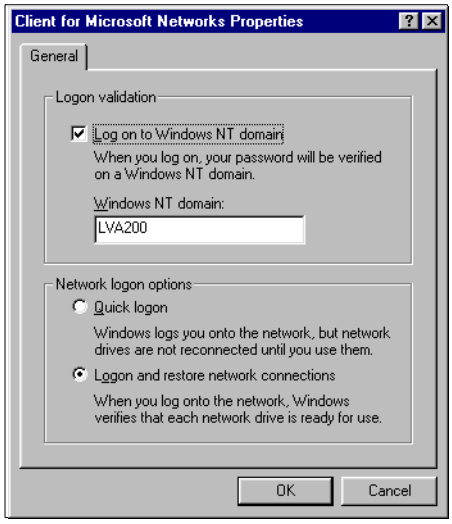


Figure 100. Client for Microsoft Networks Properties

Check the Log on Windows NT domain checkbox and enter the name of the domain as defined in the Fast Connect server. Then, press the **OK** button to confirm the change.

10.3.1 Using the Microsoft Network Client

After the configuration of the Microsoft Network Client, you should configure the profile script to meet your requirements. The startup script is located in the NETLOGON share. Its name is defined in the Fast Connect server. It can be a global, per-user, or per-computer startup script (see the startup_script parameter in Section 10.1, “Configuration of the Fast Connect server” on page 117).

You can specify both scripts, and they will both be executed at user logon. The user profile is saved on the Fast Connect server in the HOME share.

If you want to use the System Policy with Microsoft Network Client and the Fast Connect server, you must make some modifications to the registry on the Windows 95/98 client machine. Locate the following entry:
`\HKEY_LOCAL_MACHINE\System\Current Control Set\Control`.
You must correct two values in this location:

- **Update** - Change the value to 2. This value defines that the System Policy must be loaded from the NetworkPath location.

- **NetworkPath** - Enter the network path of the System Policy file on the Fast Connect server (for example `\\lva200b\netlogon\config.pol`).

Then, select **Start -> Settings -> Control Panel -> Passwords** and then select **User Profiles** tab. Check the *User can customize* box. Changes will be effective after the restart of the client.

Chapter 11. Using NetBIOS Name Server

If you do not have any WINS server in your network, you can use the AIX Fast Connect NetBIOS Name Server (NBNS) function. Name Resolution does the mapping between a NetBIOS name and its corresponding IP address. NBNS offers the WINS function except for server replication.

11.1 Configuring NBNS

You can start NBNS from the Web-based System Manager, from SMIT, or with the `net` command.

11.1.1 Setting AIX Fast Connect as an NBNS server

To start NBNS, you must click on the NetBIOS Name Server option in the Server Properties Window from Fast Connect (see Figure 101).

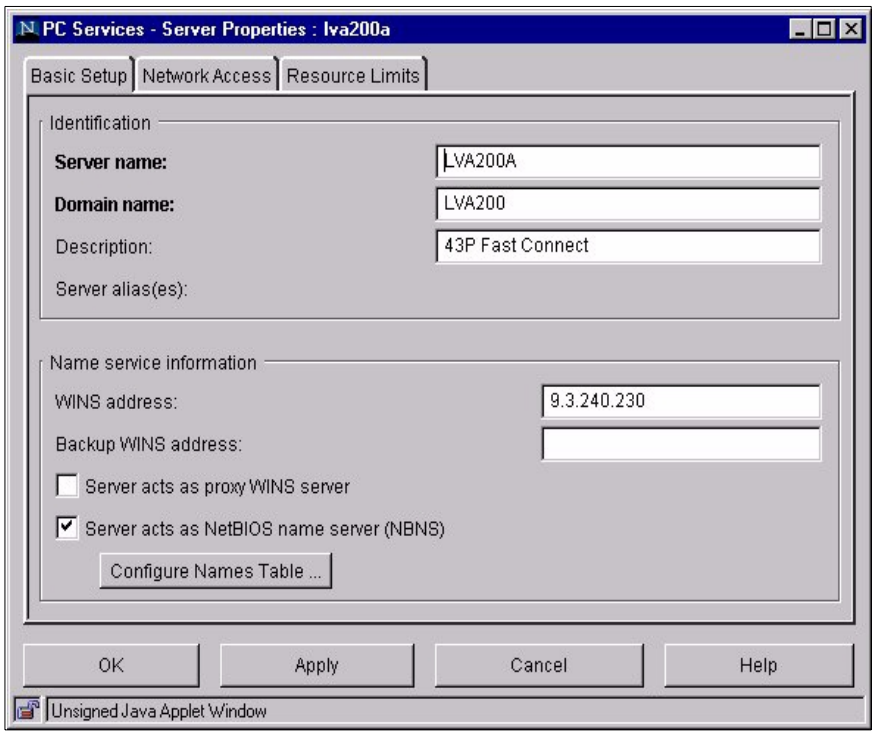


Figure 101. Fast Connect server properties

You must set the WINS Address to the loopback address (127.0.0.1) or to the local IP address of your AIX Fast Connect server (see Figure 101 on page 131). The AIX Fast Connect server uses this address to register its NetBIOS server name and resources with the NBNS server at server startup.

Use the SMIT fast path, smitty smbcfghatt.

At the command line, type `net config /nbns:1` and restart Fast Connect server.

You can check the NBNS status from the command line by entering `net nbstatus`.

You can stop NBNS from WebSM, SMIT, or at the command line by entering `net config /nbns:0`.

11.1.2 Setting AIX Fast Connect as a WINS client

When you have one or more Windows NT servers acting as a WINS server, you should avoid using the Fast Connect NBNS server (the replication to other WINS servers is not supported). You must disable NBNS and set the remote WINS server address to the IP address of Windows NT WINS server.

You should set the IP address of your primary (and secondary) WINS server on the network. AIX Fast Connect server uses this address to register its NetBIOS server name and resources with the WINS server at server startup.

You can set the WINS Address and Backup WINS Address from the Server Properties window (see Figure 101 on page 131).

Use the SMIT fast path: smitty smbcfghatt.

You can enter the following commands in any order:

- `net config /primary_wins_ipaddr:<ipaddr>`
- `net config /secondary_wins_ipaddr:<ipaddr>`

11.2 NBNS table properties

You can list, add, delete, back up, and restore the registered NetBIOS names from the NBNS table properties with Web-Based system manager, SMIT, or the `net` command.

11.2.1 Listing the NetBIOS Name Server (NBNS) table

The NetBIOS names are registered dynamically to the NBNS table.

Click on the **Configure Names Table** button from Server Properties. See Figure 102.

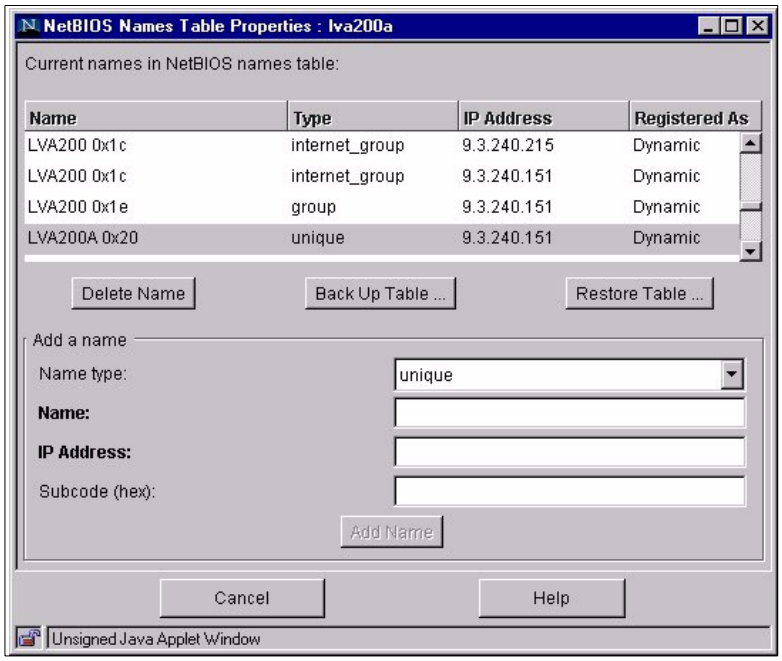


Figure 102. NetBIOS Name Table Properties

Use the SMIT fast path **smitty smbwcfgn -> List Names in NetBIOS Name table**. See Figure 103 on page 134**.**

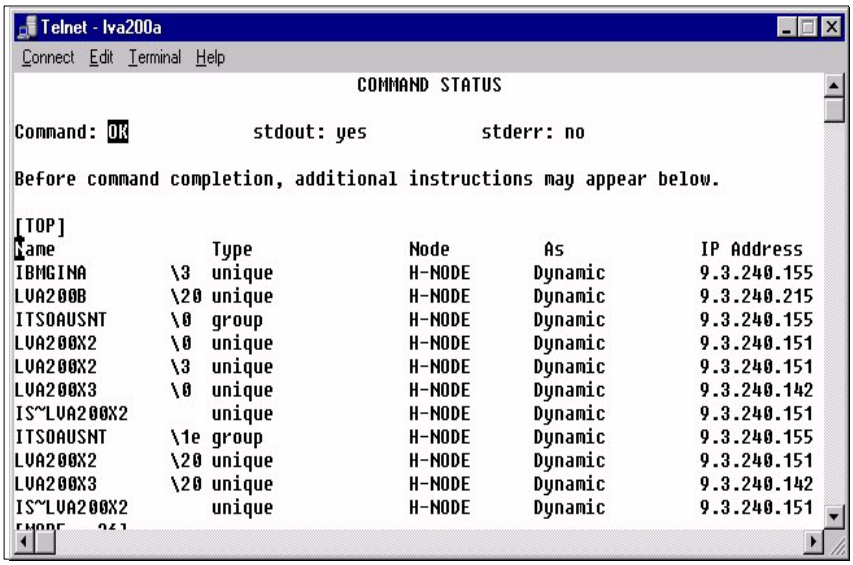


Figure 103. List of NBNS table

At the command line, type `net nblistnames`.

The NetBIOS names are saved by default in the /etc/cifs/nbnames.cur file.

The NetBIOS names are dynamically loaded in the NBNS table with the following attributes:

- **Name type**
  - **unique** - This name type is used to identify a particular host. Only one instance of a unique name can exist on any connected network.
  - **group** - This name type is referred to as a normal group in which addresses of individual members are not stored.
  - **internet_group** - This name type is a user-defined special group that stores up to 25 addresses of group members. The subcode for this type must be set to 0x1c.
  - **Multihomed** - This name type is used by hosts that have more than one interface (IP address). This name is unique to a particular host. A multihomed host can have up to 25 interfaces.
- **Name** - NetBIOS machine names can be up to 16 characters long. The first 15 characters of a NetBIOS name can be specified by the user or administrator, but the 16th character is reserved (00-FF hex) to specify a resource type. The following are examples of some codes that are used:

- **00** Workstation service (computer) name.
- **1B** Domain master browser name.
- **1C** Domain group name.
- **1D** Master browser name.
- **1E** Normal group name, it is used by the browsers to elect a Master Browser.
- **20** This is the server service name used to provide share point for file or print sharing.

- **Node** - There are four NetBIOS over TCP/IP name resolution methods, b-node, p-node, m-node, and h-node. For the description of each type of node, see Section 1.2, “Types of nodes” on page 2.
- **IP address** - This is the IP address of machine name.

11.2.2 Adding a static name

Names added manually to the NBNS table are considered *static* names, and you do not need to refresh them.

You can add a NetBIOS name to the NBNS table (see Figure 102 on page 133).

Use the SMIT fast path, smitty smbwcfgn -> ADD a NetBIOS Name (see Figure 104 on page 136).

You can choose between four Name Types:

- unique
- group
- multihomed
- internet_group

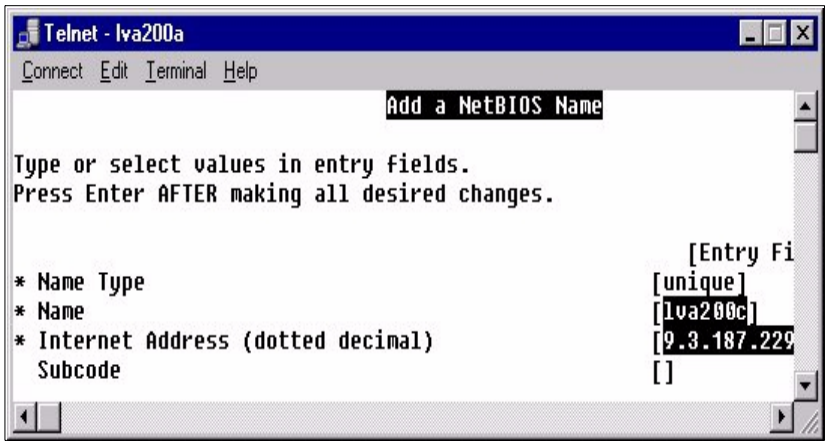


Figure 104. Add a NetBIOS Name

For a permanent NetBIOS unique name, at the command line, type

```
net nbaddname /name:<name> /ipaddress:<ipaddress> /sub:<val>
```

For a permanent NetBIOS group name, at the command line, type

```
net nbaddgroup /name:<name> /ipaddress:<ipaddress> /sub:<val>
```

For permanent NetBIOS multihomed name, at the command line, type

```
net nbaddmulti /name:<name> /ipaddress:<ipaddress> /sub:<val>
```

For permanent NetBIOS Internet group name, at the command line, type

```
net nbaddingrp /name:<name> /ipaddress:<ipaddress> /sub:<val>
```

In the NetBIOS table, you will see that the new name is added as static; this means that the name cannot be deleted by any client machines, but must, instead, be deleted using the delete name option on the Fast Connect server.

Note

If you add a static entry to the NBNS table with a Name Type as internet_group, you must define a subcode of 0x1C. The subcode is the last byte of the NetBIOS name. The subcode value is optional for all name types except internet_group.

11.2.3 Deleting an entry from the NBNS table

You can delete NetBIOS names from an NBNS table with WebSM, SMIT, or the `net` command. You can delete a NetBIOS name by name or by name and address (see Figure 105).

11.2.3.1 Deleting a NetBIOS Name by name

You can use SMIT and type `smitty smbwcfgdel`.

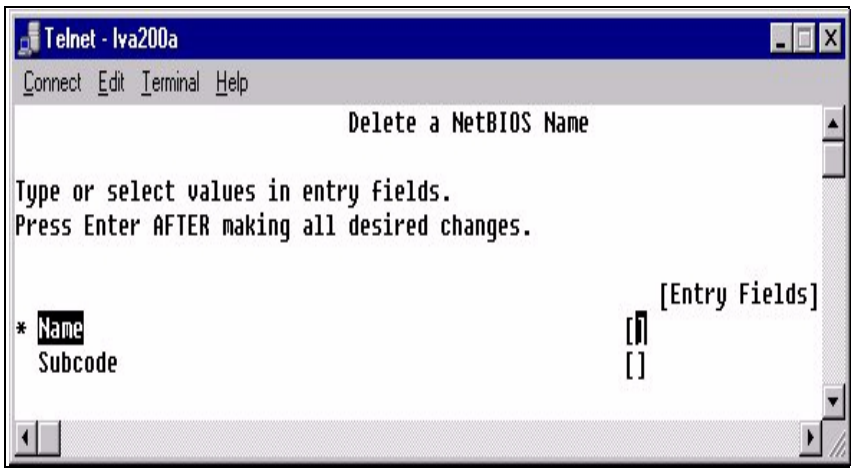


Figure 105. Delete a NetBIOS Name

At the command line, type: `net nbdelname /name:<name> /sub:<subcode>`

11.2.3.2 Deleting by Address and by Name

You have to use this option if you want to delete an Internet group name only. If there is more than one IP address associated with the Internet group name, only this IP address will be deleted from the NBNS table. See Figure 106 on page 138.

Using SMIT, type `smitty smbwcfdadd`.

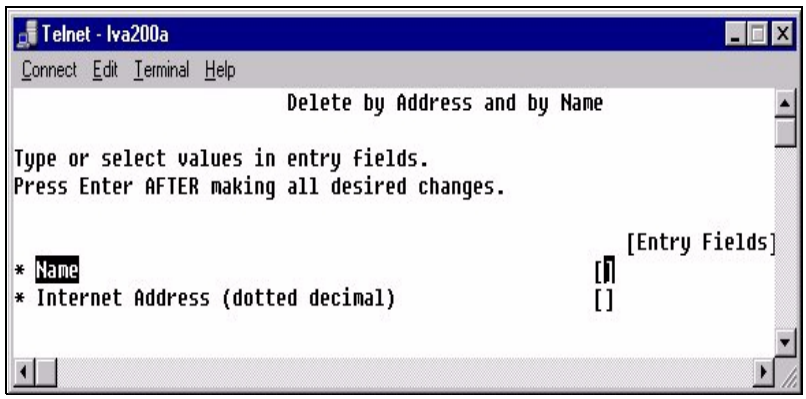


Figure 106. Delete by Address and by Name

Enter the following at the command line:

```
net nbdeladdr /name:<name> /ipaddress:<ipaddress>.
```

11.2.4 Backup/restore of the NBNS table

You can save the NBNS table in a text file and restore it later. Then, if NBNS goes down, you can restore your environment more quickly (see Figure 102 on page 133). The names are written to the following default file: /etc/cifs/nbns.names. If you want to change this default path, you have to specify a fully-qualified filename with the path.

Use the SMIT fast path:

- For backup: `smitty smbwcfgbak`
- For restore: `smitty smbcfgres`

At the command line, type:

- `net nbbackup /name:<filename>`
- `net nbrestore /name:<filename>`

Note

If you restore the NBNS table, it will not overwrite the old entry in the table but add the new NetBIOS name to the list of the table.

11.3 WINS Proxy Server

You can configure the AIX Fast Connect server as a WINS Proxy server. That means that the server can resolve name queries for non-WINS-enabled clients. Non-WINS-enabled clients use the Broadcast Node (b-node) protocol for name queries.

When a WINS Proxy server receives a request from a client, it first checks for the requested name in its cache. If the name is not in its cache, Fast Connect sends the name resolution request to its WINS server.

You can set this WINS Proxy function in the Server Properties window (see Figure 107).

Use the SMIT fast path, smitty smbcfghatt.

At the command line, type `net config /wins_proxy:<0 | 1>`.

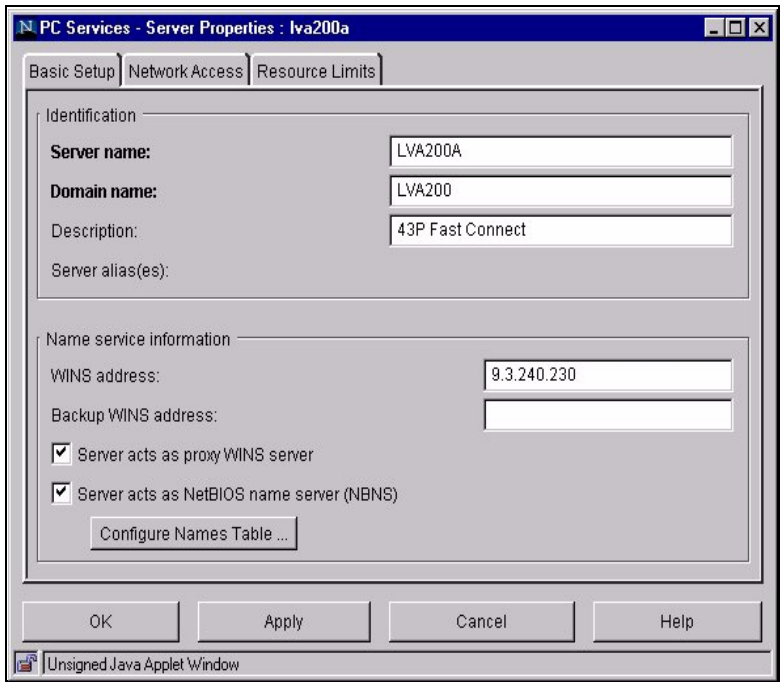


Figure 107. Fast Connect server properties

The following sections describe two experiments demonstrating the proxy WINS server function.

11.3.1 First experiment

We set up the RISC/6000 43P as a Fast Connect server with only a proxy WINS server setting an F50 that acts as a WINS server and PC clients (see Figure 108 on page 140).

The PC client is not configured for WINS resolution; it acts as b_node.The F50 and 43P are h_node.

In this example, a NetBIOS application on PC client wishes to communicate with the F50 Fast Connect server. Normally, this would not be possible, but, by using the 43P as a proxy WINS server in the same LAN as our PC client, the PC client and the F50 can communicate.

The PC client wants access to a shared resource on F50. The PC client broadcasts a Name Query Request on the local network to obtain the IP address of F50. The F50 does not receive the broadcast request because it cannot cross the router.

The proxy WINS server (43P) sees the name query broadcast for a node on a different subnet. It checks for the requested name in its NBNS cache and finds the IP address of F50. Then, it sends a positive Name Query response containing the IP address of the F50 to the PC client.

The PC client now has the IP address of the F50 and can access the shared resources on the F50 Fast Connect server. See Figure 108.

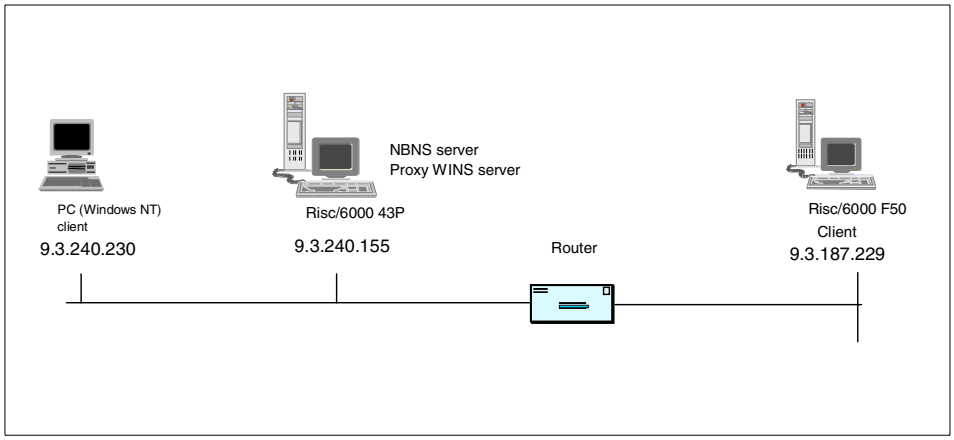


Figure 108. Proxy WINS Server (43P) as NBNS server and proxy WINS server

11.3.2 Second experiment

The PC1 client is not configured for WINS resolution. It acts as b_node. The RISC/6000 43P is configured as a Proxy WINS server, and The F50 is configured for WINS client resolution. The PC2 is configured as a WINS server (see Figure 109 on page 141).

The F50 and 43P are h_node and configured as Fast Connect server.

In this example, a NetBIOS application on PC1 wishes to communicate with the F50 Fast Connect server. Normally, this would not be possible. But, by using the 43P as a proxy WINS server in the same local network as the PC1 client, the PC1 client and F50 can communicate.

43P and F50 are registered on the PC2 WINS server. From PC1 client, we want to access shared resources on F50. PC1 broadcasts a Name Query request on the local network to obtain the IP address of the F50 Fast Connect server. The F50 does not receive the broadcast because of the router.

The proxy WINS server (43P) sees the name query broadcast for a node on a different subnet. It checks his or her cache table, and the name cannot be found. Then, it sends a Name Query request directed datagram to the WINS server (PC2). PC2 returns a positive Name Query Response containing the IP address for F50 client to the proxy server.

Then, the proxy WINS server sends a datagram to PC1 client with the IP address for the F50 Fast Connect server. PC1 and F50 can now communicate. See Figure 109.

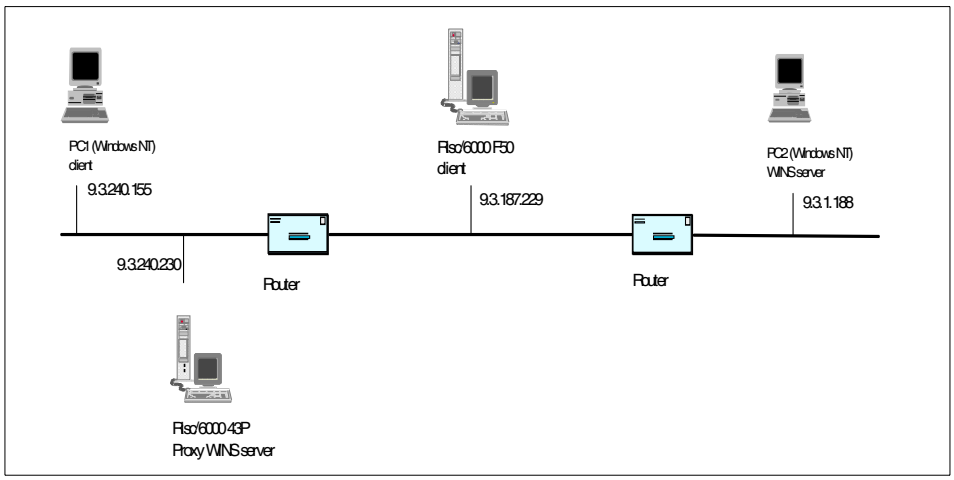


Figure 109. Proxy WINS server

Chapter 12. Sizing guidelines

Every system will reach a bottleneck at a certain level of performance. Some bottlenecks are easy to predict, a type of network cable can only transfer data up to its specified rate. Other bottlenecks are harder to predict, interactions between client and server, such as file size and client activity.

In order to reach 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 needs to handle the planned transaction workload. All workloads are made up of:

- 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 to 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 the resources and time we had were limited, we decided to focus our experiments on activities that were very specific to the Fast Connect product. 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 sizing factors: CPU, memory, and network.

12.1 Practical experimentation

Since we had neither all the equipment in our lab required to connect thousands of users nor hundreds of users to enter commands on the keyboard, we had to find an alternate way of simulating user connections. What we have done is 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 clients 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 started a thousand requests at the same time and observed the behavior of the system. The first result showed that this was not convincing and perhaps a bit far from reality. The second version of our test allowed us to start the same thousand requests, but spread evenly over one minute, which seems to better reflect reality. We then developed eight sets of scripts:

- This test simulates a given number of clients that connect to the server within a minute, wait some time, and then disconnect from the server. The reason for this delay is that disconnection also uses some CPU and we do not 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 performed by the Fast Connect server using the /etc/cifs/cifsPasswd file
  b. Remote authentication using a Microsoft Windows NT Primary Domain Controller

- This test simulates a given number of users connecting to the server, changing directories, and listing the files in the new directory.
- 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.
- This test simulates a given number of users connecting to the server and getting a 10 KB file. The reasons for such a small file are to measure the CPU associated with the retrieval of the file and to avoid being impacted by I/O or Network bottlenecks.
- This test simulates a given number of users connecting to the server and putting a 10 KB file. The reasons for such a small file are to measure the CPU associated with the retrieval of the file and to avoid being impacted by I/O or Network bottlenecks.
- This test simulates a given number of users connecting to the server and printing a 10 KB file. The reasons for such a small file are to measure the CPU associated with the retrieval of the file and to avoid being impacted by I/O or Network bottlenecks. Also, we have created a dummy print queue, because, afterwards, it was quite hard to distinguish between the CPU load from the Fast Connect server and the print server. The CPU and 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.
- 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.
- This test studies the transfer of large file, where I/O and network becomes the bottleneck. We simulate a given number of users transferring a 10 MB file from the client to the server.

These 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 scripts are launched from a remote RS/6000, and we also run the `vmstat` command on this client machine to make sure that it doesn't become a bottleneck in our experiment.

12.1.1 Results

With these tests, we are recording the impact on the server using the `vmstat` commands. The results we get are: The number of refused connections (when the Fast Connect server becomes too busy, it refuses new connections), the time used to perform an operation, such as connecting,

browsing, getting, putting, and printing a file, as well as the average CPU load on the server during that operation.

12.1.2 RS/6000 43P-150

The first machine tested was an RS/6000 43P-150. The machine was used to simulate the clients is a four-way F50.

12.1.2.1 Configuration

The machine is a uniprocessor 43p150 with a 375 Mhz 604e processor card. It has 512 MB of RAM and two 4.5 GB disks. The operating system is 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 is 4.3.3 and Fast Connect is at level 2.1.1.12 for cifs.basic.rte and 2.1.1.10 for cifs.base.cmd.

12.1.2.2 Results

Figure 110 shows the number of connections refused as the number of connections attempted increases.

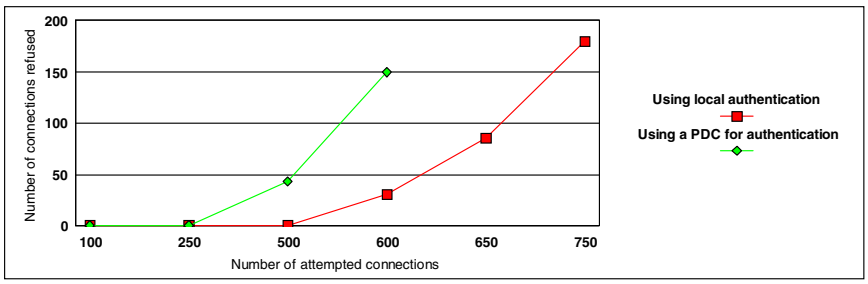


Figure 110. Number of refused connections

Figure 111 on page 147 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.

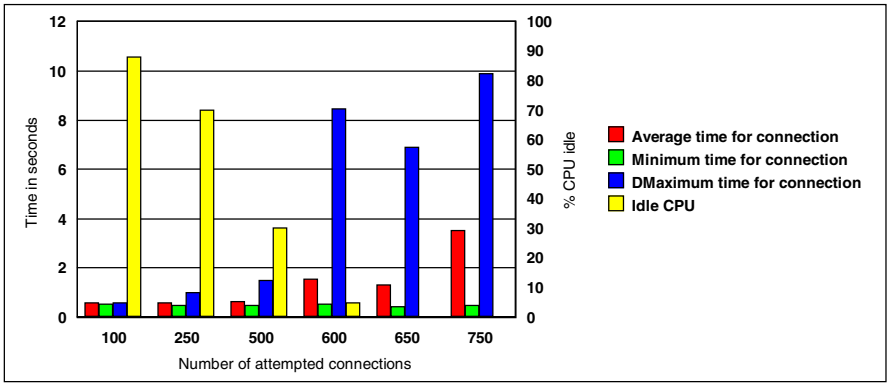


Figure 111. Time required per connection

Figure 112 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.

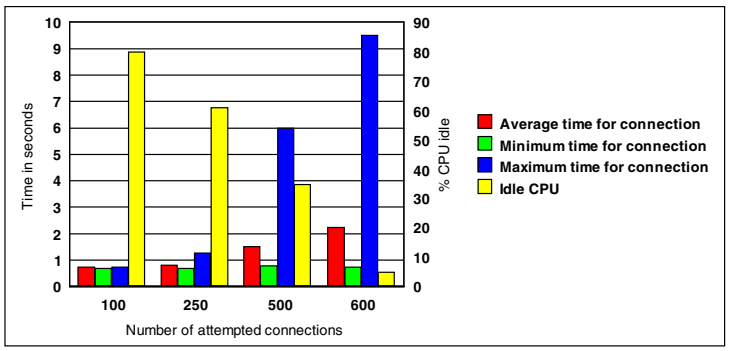


Figure 112. Time required per connection when authenticating to a PDC

Figure 113 on page 148 shows the time it takes to connect to a server and change directory (as a function of the number of attempted connections) and the associated CPU load on the server.

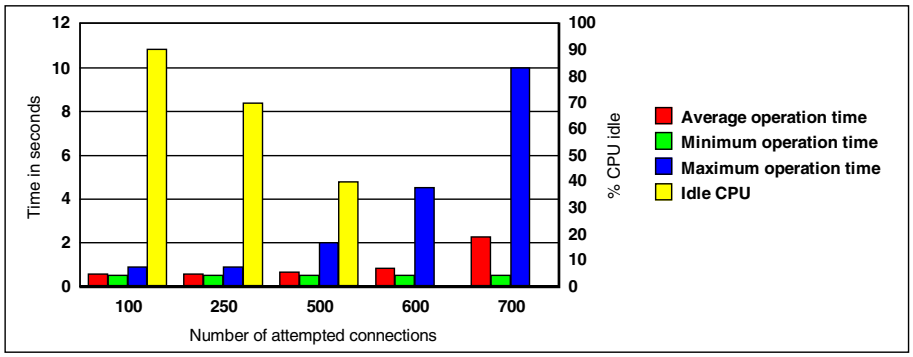


Figure 113. Time required to connect and change directory

Figure 114 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.

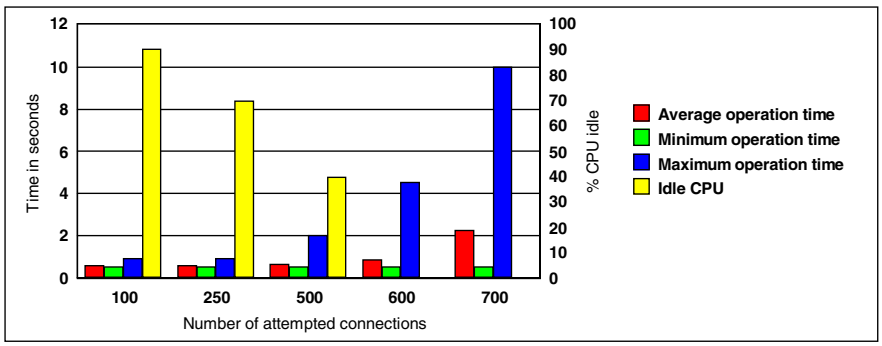


Figure 114. Time required to connect and browse file

Figure 115 on page 149 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.

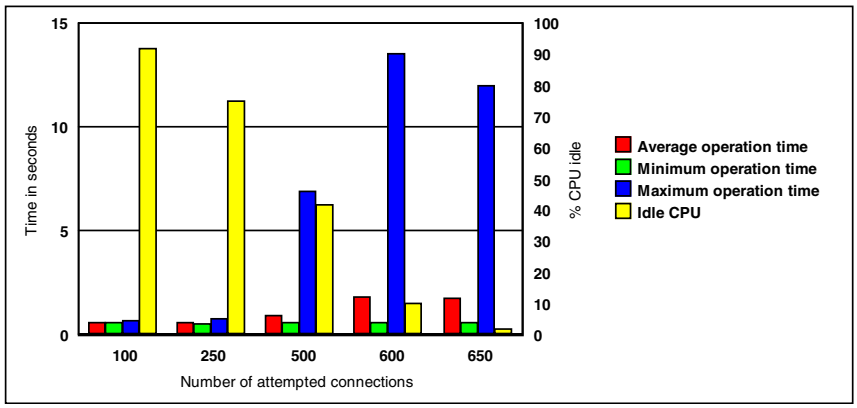


Figure 115. Time required to connect and get a 10 KB file

Figure 116 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.

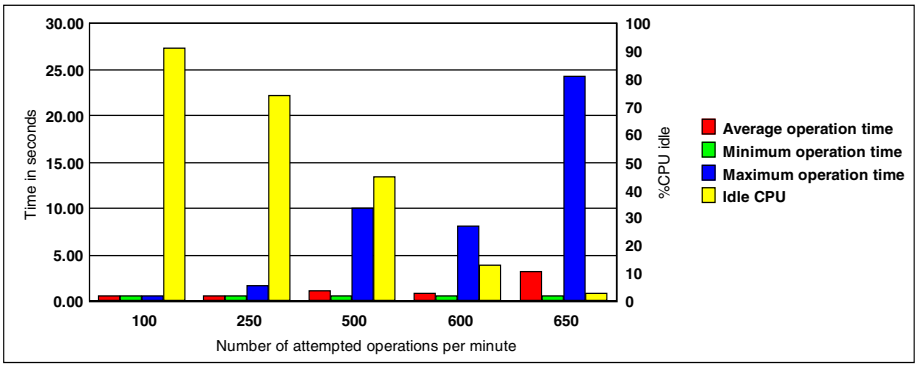


Figure 116. Time required to connect and put a 10 KB file

Figure 117 on page 150 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.

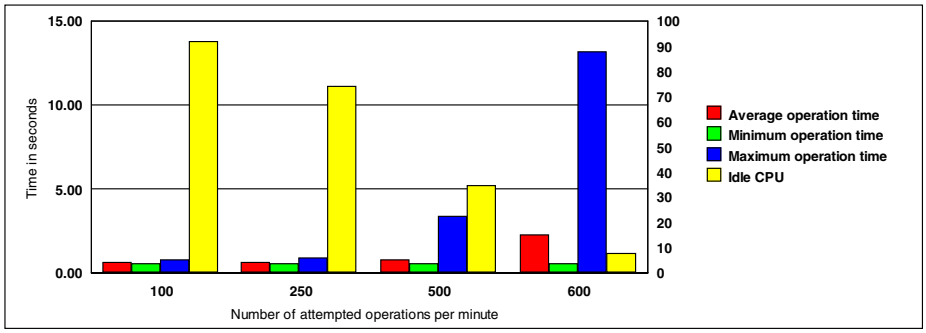


Figure 117. Time required to connect and print a 10 KB file

Figure 118 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.

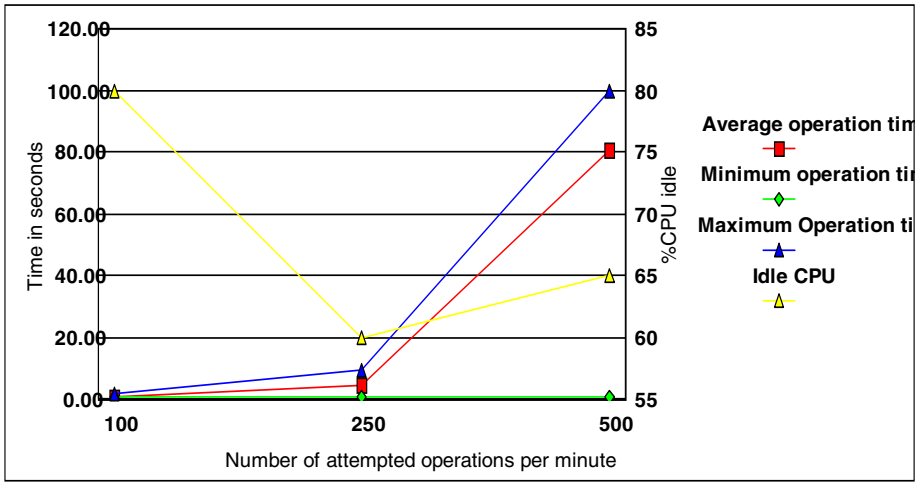


Figure 118. Time required to connect and transfer a 10 MB file

12.1.3 RS/6000 43P-260

The first machine tested was an RS/6000 43P-260. The machine used to simulate the clients was a four-way F50.

12.1.3.1 Configuration

The machine is a two-way 43p260 with 200 Mhz POWER3 processors. It has 2 GB of RAM and two 4.5 GB disks. The operating system was installed on

the first disk, and our experience data was on the second disk (no mirrored or striped logical volumes). It also had a Token Ring adapter.

The version of AIX is 4.3.3 and Fast Connect is at level 2.1.1.12 for cifs.basic.rte and 2.1.1.10 for cifs.base.cmd.

12.1.3.2 Results

Figure 119 shows the number of connections refused as the number of connections attempted increases.

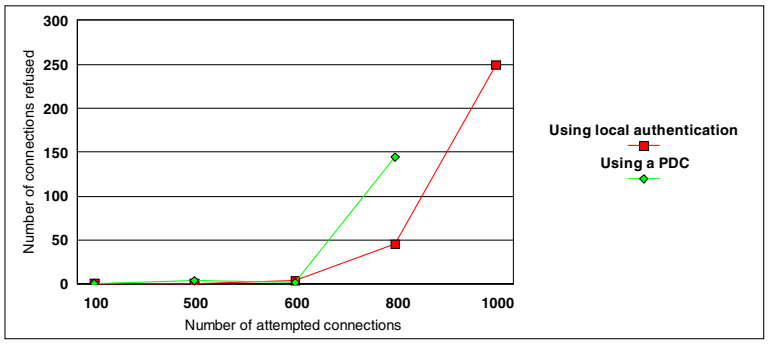


Figure 119. Number of refused connections

Figure 120 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.

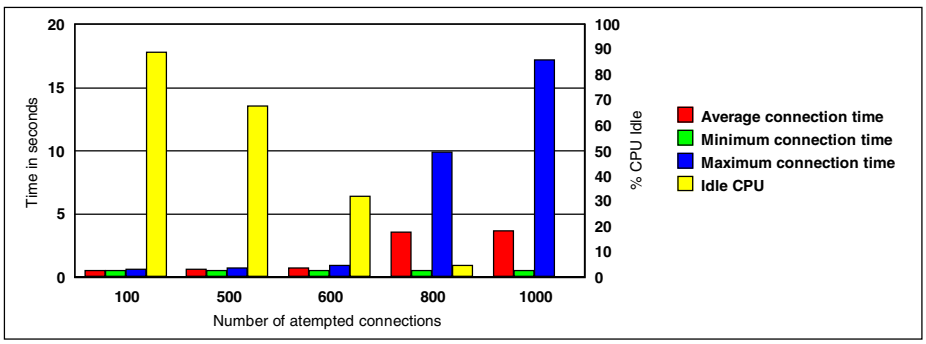


Figure 120. Time required per connection

Figure 121 on page 152 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.

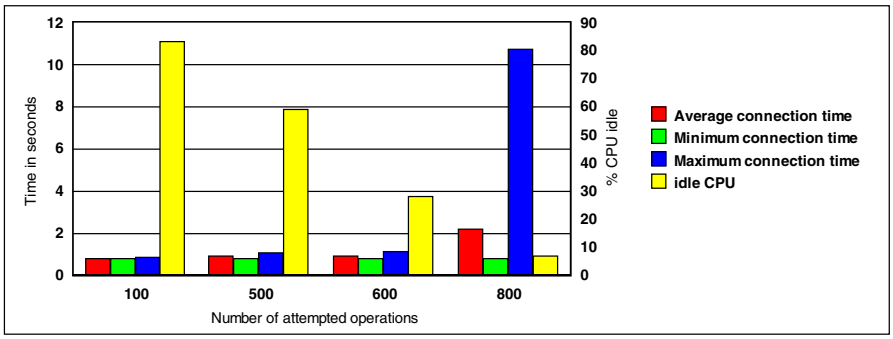


Figure 121. Time required per connection when authenticating to a PDC

Figure 122 shows the time it takes to connect to a server and change the directory (as a function of the number of attempted connections) and the associated CPU load on the server.

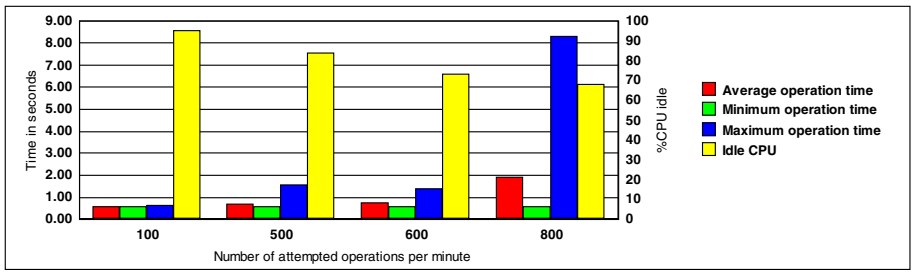


Figure 122. Time required to connect and change directory

Figure 123 on page 153 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.

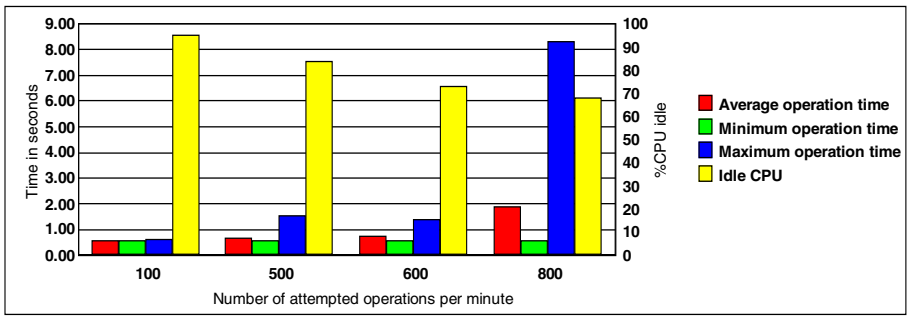


Figure 123. Time required to connect and browse file

Figure 124 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.

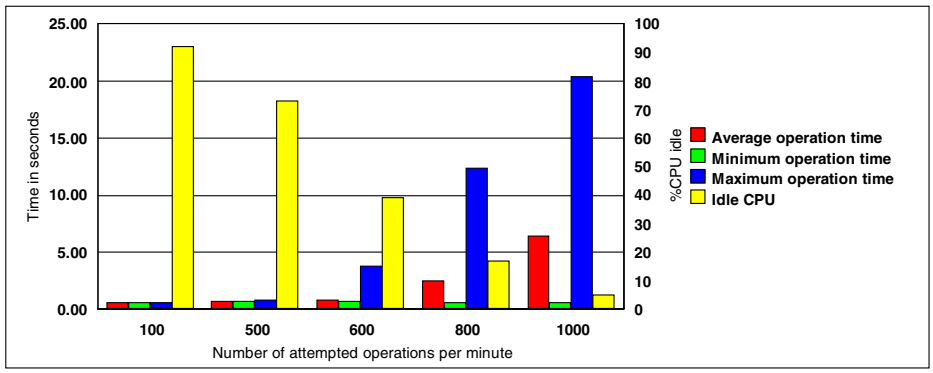


Figure 124. Time required to connect and get a 10 KB file

Figure 125 on page 154 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.

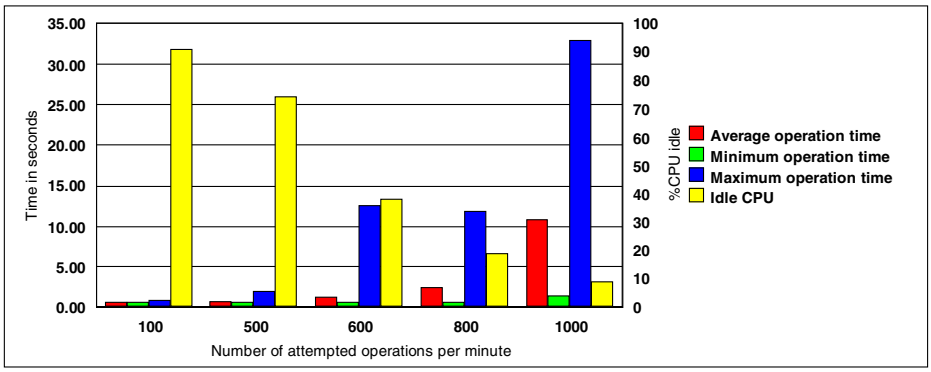


Figure 125. Time required to connect and put a 10 KB file

Figure 126 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.

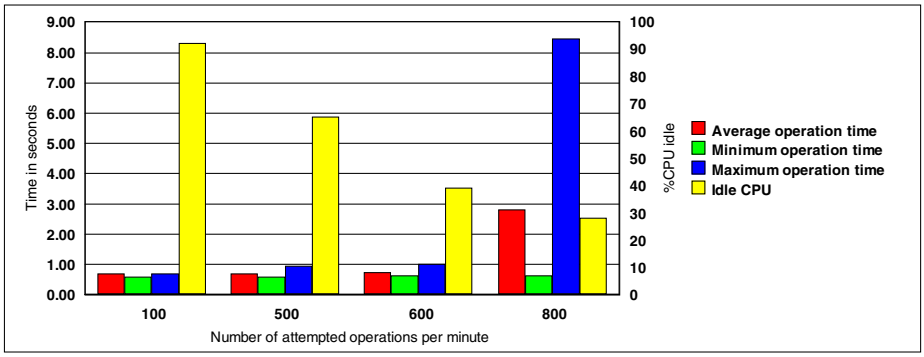


Figure 126. Time required to connect and print a 10 KB file

Figure 127 on page 155 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 results.

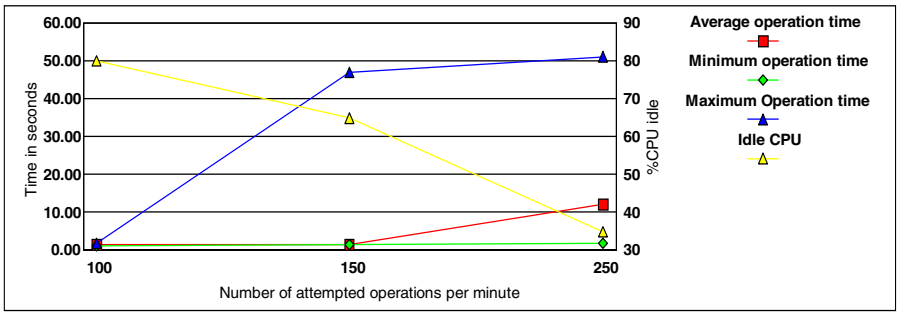


Figure 127. Time required to connect and transfer a 10 MB file

12.1.4 RS/6000 four-way F50

The third machine tested was an RS/6000 F50. The machine used to simulate the clients was a 12-way S7A.

12.1.4.1 Configuration

The machine is a four-way F50 with 332 Mhz 604e processors. It has 2 GB of RAM, two 4.5 GB disks. The operating system was installed on the first disk, and our experience data was 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 Fast Connect is at level 2.1.1.12 for cifs.basic.rte and 2.1.1.10 for cifs.base.cmd.

12.1.4.2 Results

Figure 128 on page 156 shows the number of connections refused as the number of connections attempted increases.

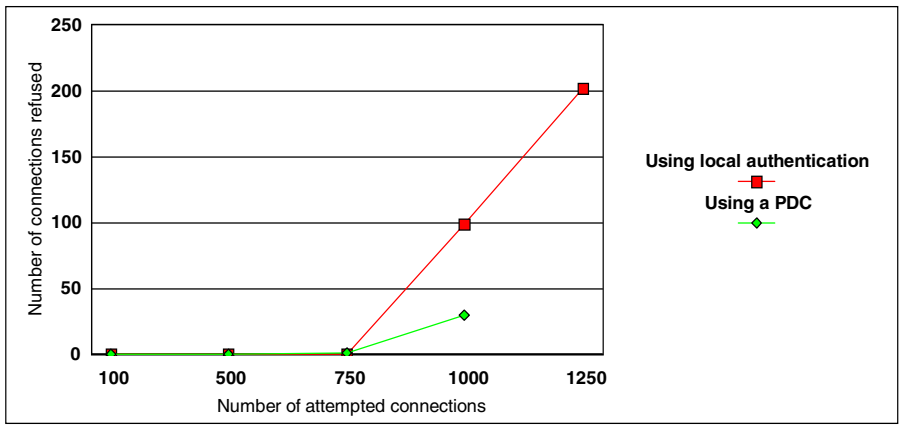


Figure 128. Number of refused connections

Figure 129 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.

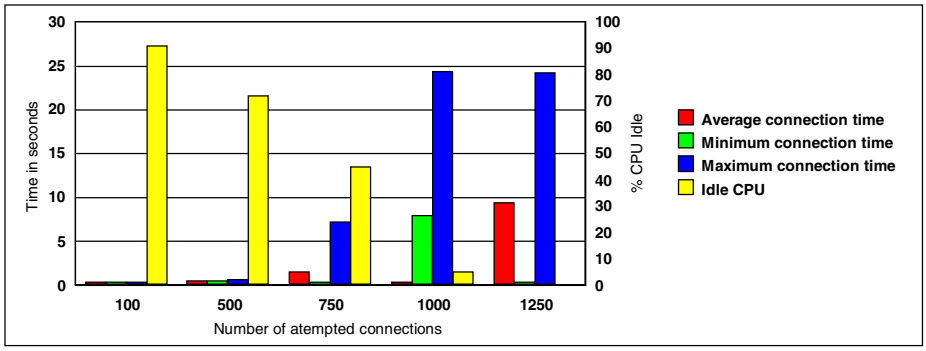


Figure 129. Time required per connection

Figure 130 on page 157 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.

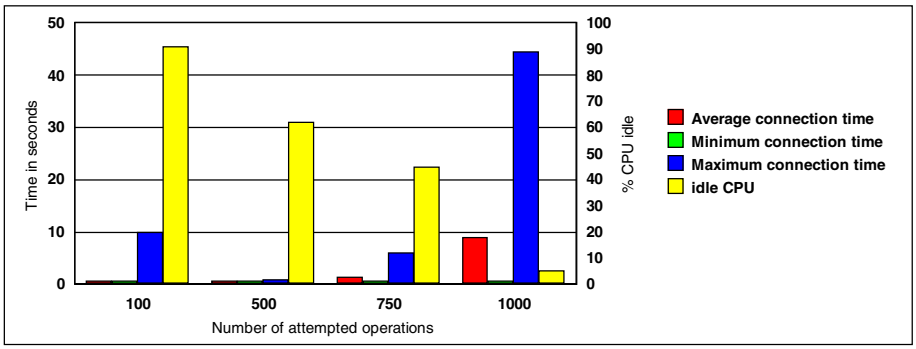


Figure 130. Time required per connection when authenticating to a PDC

Figure 131 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.

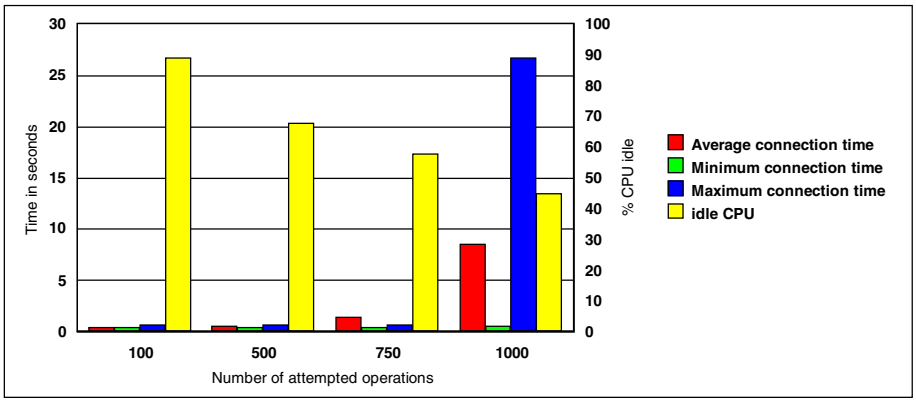


Figure 131. Time required to connect and change directory

Figure 132 on page 158 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.

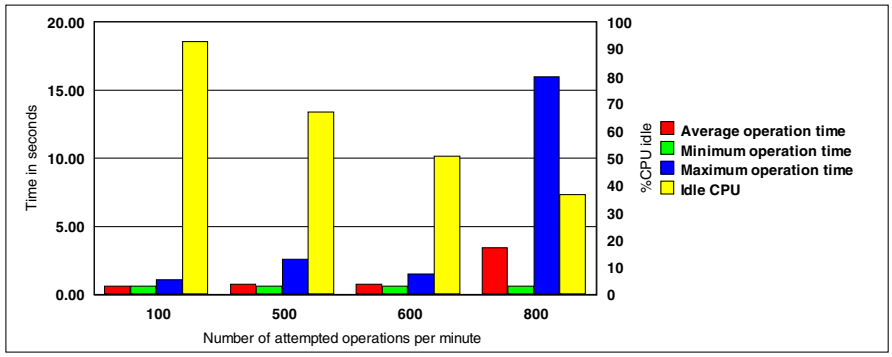


Figure 132. Time required to connect and browse file

Figure 133 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.

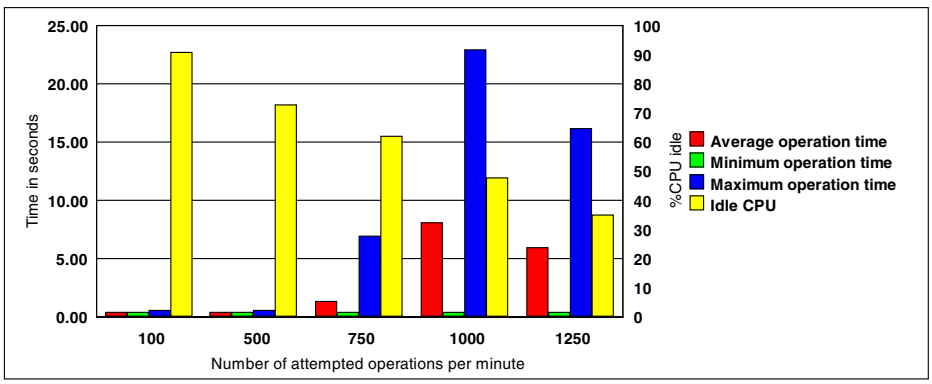


Figure 133. Time required to connect and get a 10 KB file

Figure 134 on page 159 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.

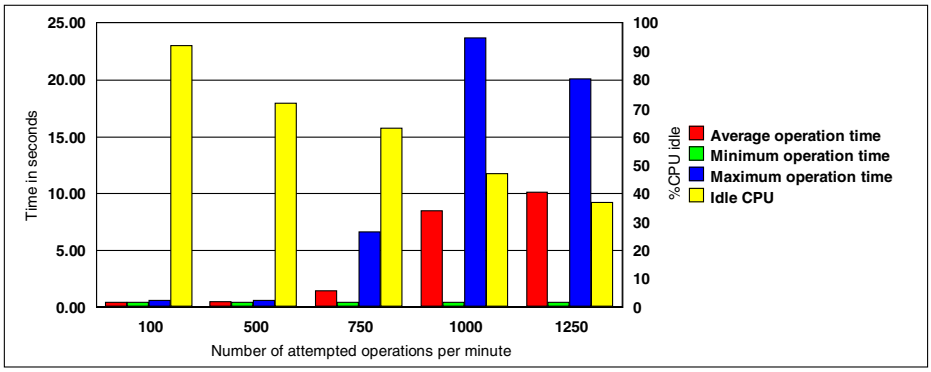


Figure 134. Time required to connect and put a 10 KB file

Figure 135 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.

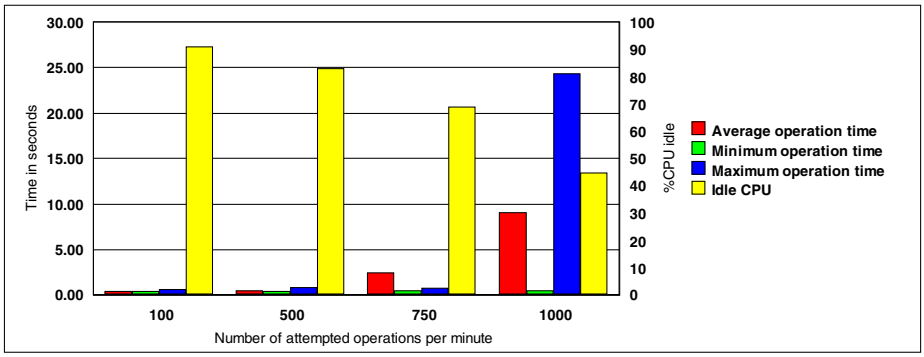


Figure 135. Time required to connect and print a 10 KB file

Figure 136 on page 160 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 results.

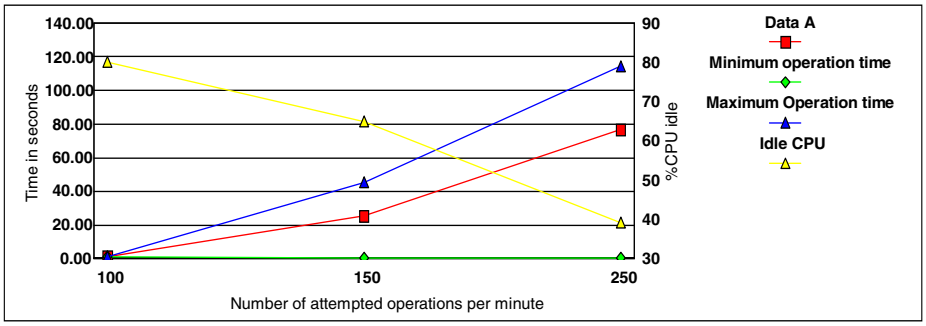


Figure 136. Time required to connect and transfer a 10 MB file

12.1.5 RS/6000 12-way RS/6000 S7A

The last machine 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 too many connections, and we didn't have any machine powerful enough to act as a client; so, we used three systems as the client: The F50, the 43P260, and a J50 (a four-way 120 MHz 604 processor), and we spread the load over 30 seconds instead of one minute.

12.1.5.1 Configuration

The machine was a 12-way S7A with 262 Mhz RS64 II processors. It had 1 GB of RAM and 11 4.5 GB disks. The operating system was installed on the first disk, and our experience data was on the other disks (no mirrored or striped logical volumes). It also had a Token Ring adapter.

The version of AIX is 4.3.3, and Fast Connect is at the level 2.1.1.12 for cifs.basic.rte and 2.1.1.10 for cifs.base.cmd.

12.1.5.2 Results

Figure 137 on page 161 shows the number of connections refused as the number of connections attempted increases.

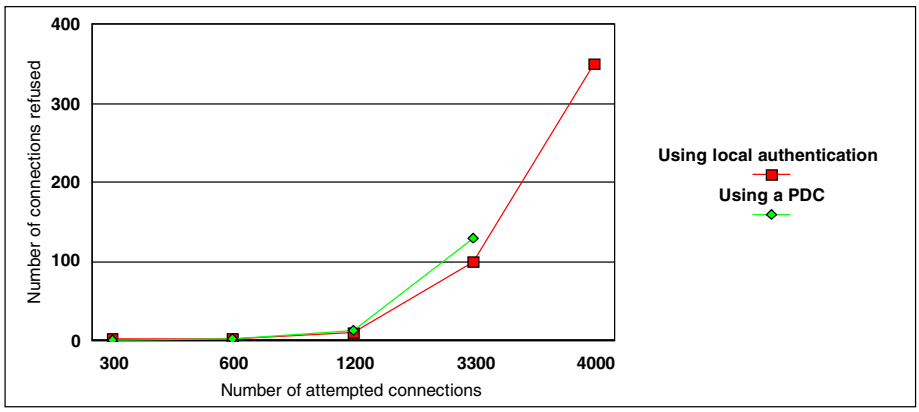


Figure 137. Number of refused connections

Figure 138 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.

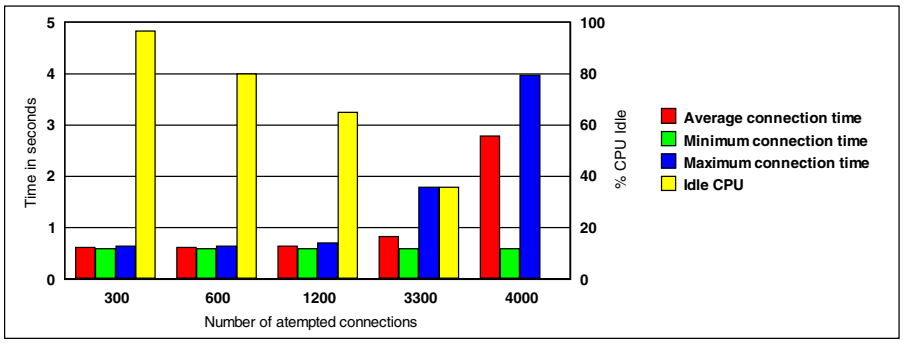


Figure 138. Time required per connection

Figure 139 on page 162 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.

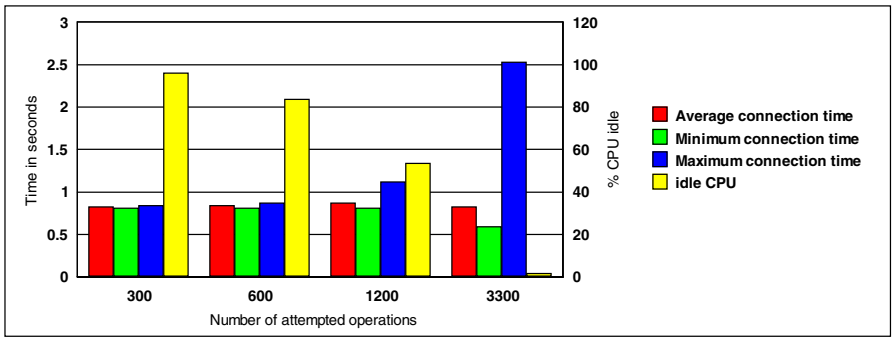


Figure 139. Time required per connection when authenticating to a PDC

Figure 140 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.

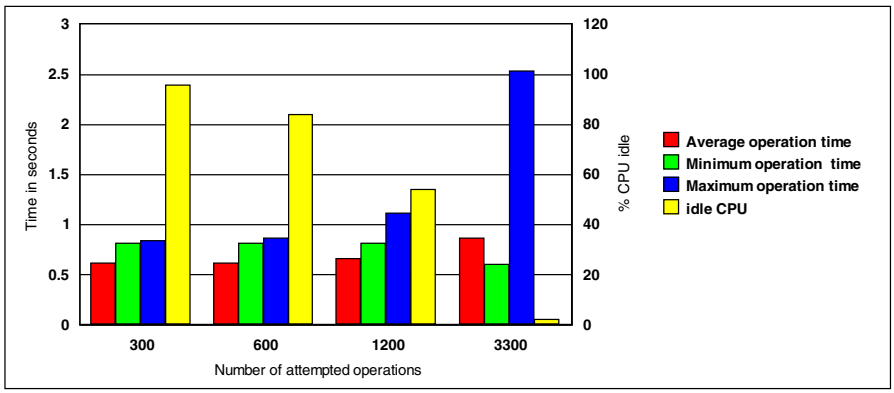


Figure 140. Time required to connect and change directory

Figure 141 on page 163 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.

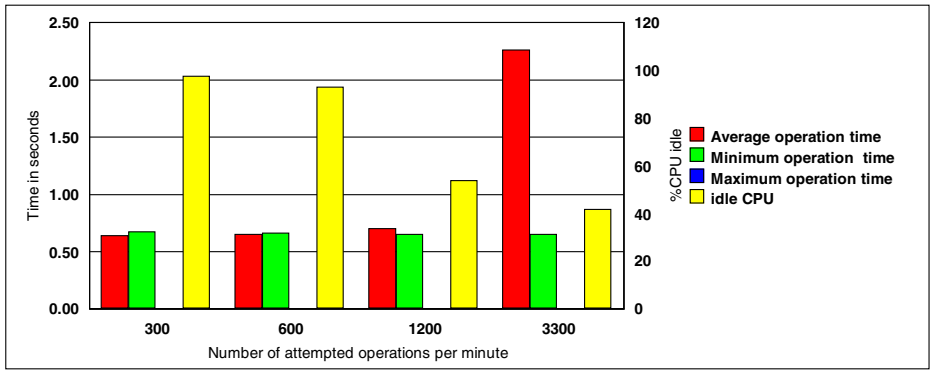


Figure 141. Time required to connect and browse file

Figure 142 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.

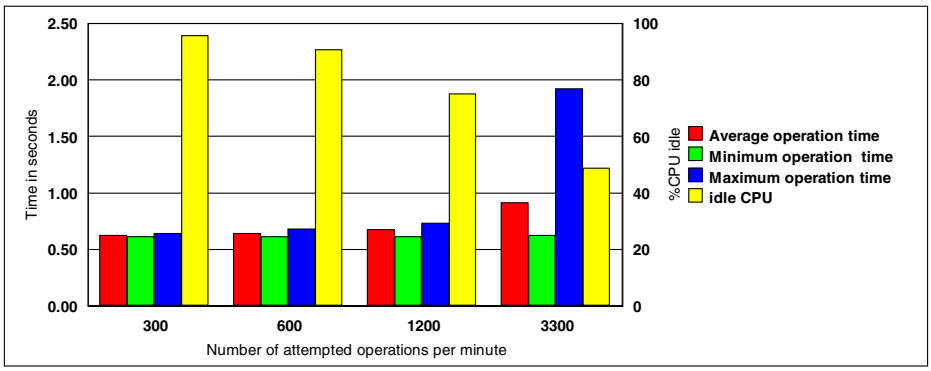


Figure 142. Time required to connect and get a 10 KB file

Figure 143 on page 164 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.

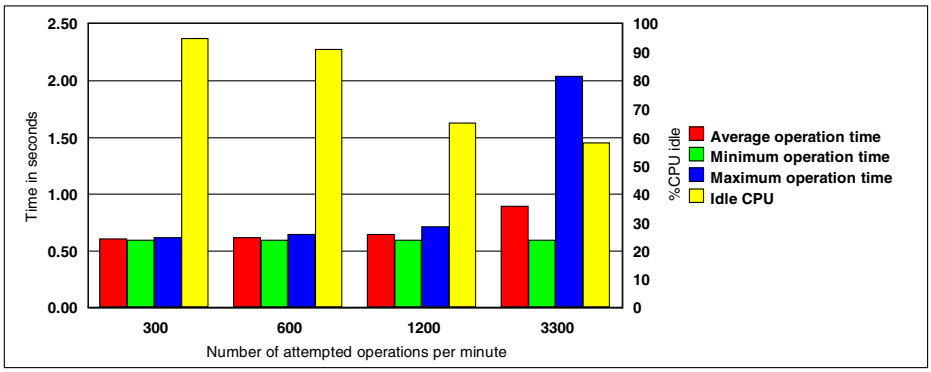


Figure 143. Time required to connect and put a 10 KB file

Figure 144 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.

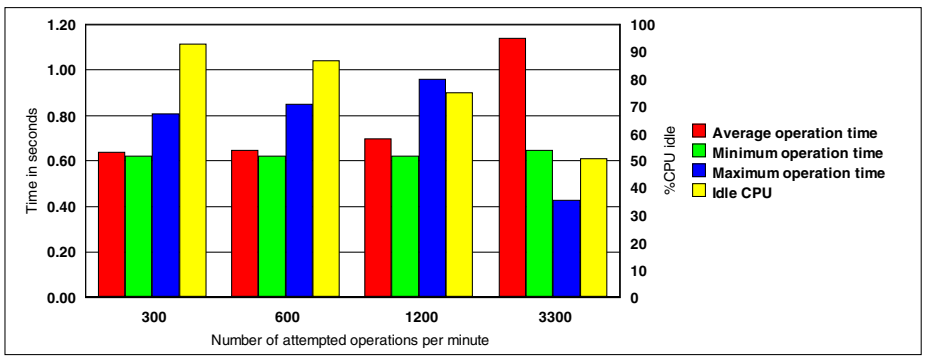


Figure 144. Time required to connect and print a 10 KB file

Figure 145 on page 165 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 results.

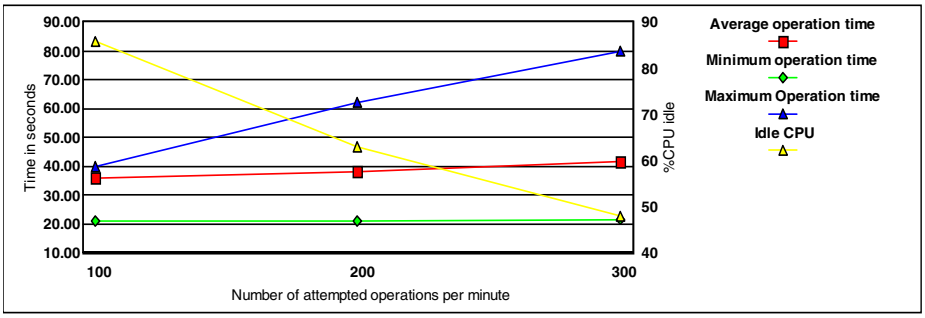


Figure 145. Time required to connect and transfer a 10 MB file

12.1.6 Conclusion

At the end of these tests, there are some conclusions that can be extracted from these numbers. Let us start with the easy ones.

12.1.6.1 Memory sizing

The reading of the result of the `vmstat` commands confirms the developers design. To every connecting user, there is associated a new thread and a new process. 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. In addition, 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.

12.1.6.2 Network sizing

Sizing the network is usually a complex task, the only goal we had during this experimentation was to make sure that using Fast Connect 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 great impact on the network. The transfer rates observed during the get and put operations for big files show that we reached the nominal bandwidth of the network; so, the choice of the network must be made based on the expected network traffic. Fast Connect does not add any overhead.

12.1.6.3 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

term of CPU, is the login-authentication part. This is where we saw the limitation of the percentage of idle CPU being 0 percent and having a system that would not respond anymore. Table 2 gives the maximum number of users that can connect within a minute for each of the systems tested.

Table 2. Maximum number of users connecting within one minute

43P150	43P260	F50	S70
500	800	1100	3500

Of course, the maximum number of users for the system will be limited by the total amount of memory. 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 1800 users logged, that is:

(RAMSIZE - MEMOS) / SIZEPERUSER

Where

RAMSIZE = Amount of memory on your system
MEMOS = Amount of memory required by the base operating system with all the applications running (the base operating system that could be up to 100 MB)
SIZEPERUSER = 0.5 each Fast Connect user requires 0.5 MB.

The amount of time needed to log these users is given by the number of users divided by the maximum number of users that the system can log per minute. For our 43P-150, the time needed to log on 1800 users would be 1800/ 500 = 3.6minutes (500 is shown in Table 2 as the maximum number of users logged in a minute for the 43P).

You could log more users than that, but, after this point, you will start paging and, then, the response time will increase drastically.

The login/authentication step is the heaviest. The other step studied during our test never caused the system to be 100 percent full, but, once again, the test 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 of this writing, 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 of them at `http://www.redbooks.ibm.com/portals/rs6000`.

Appendix A. Troubleshooting

This section describes the basic tools for locating the problems with the Fast Connect server, clients, and the SMB/CIFS protocol and how to narrow them down.

A.1 Protocol levels

It is difficult 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 that you should remember when troubleshooting the SMB protocol.

TCP/IP is a protocol divided into separated independent levels. This architecture helps us because, normally, we only have a problem in one level and we 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. For example, if you have a problem with name resolution, the access to the shares will probably not work.

- **TCP/IP protocol**
  - **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 protocol**
  - **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 The Fast Connect server environment

The AIX Fast Connect server can be in one of the following three states:

not running This is the *not active* state before you load and start the server.

paused This is the state where the server is not accepting connections from new clients. All existing connections are still active.

running This is the active state when the server is accepting connections.

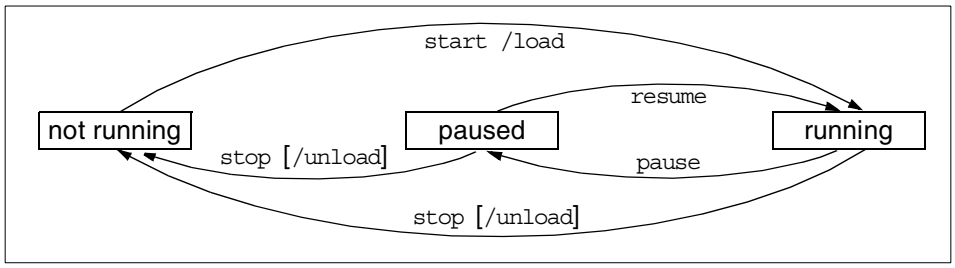


Figure 146. AIX Fast Connect server states

If you decide to start the server automatically after reboot, AIX Fast Connect installation inserts one line into the /etc/inittab:

```
rccifs:2:wait:/etc/rc.cifs start > /dev/console 2>&1
```

If you do not want to start the AIX Fast Connect server automatically after reboot, you should delete (or better yet, comment out) this line from the /etc/inittab file.

You should also use /etc/rc.cifs start instead of net start for a normal (re)start of the server because the script, rc.cifs, also set environmental variables that can increase the performance of the server.

The /etc/rc.cifs script starts the AIX Fast Connect server, and then you can see the following processes running:

```
$ ps -fel | grep -v grep | grep cifs
    root 20186     1   0 11:49:56      -  0:00 /usr/sbin/cifsServer
    root 22904     1   0 11:49:56      -  0:00 /usr/sbin/cifsPrintServer
```

If you have the AIX Fast Connect Advanced server version, you will see cifsServAdv instead of the cifsServer process. AIX Fast Connect server is a multi-threaded application; so, you will see only one process all the time. You can also see the cifsUser process for each connection. The printer server is not multi-threaded; so, you will see at least one process and, in addition, one for every print client connection.

The configuration files for the server are located in the /etc/cifs directory. The configuration file for the server is a plain text file, cifsConfig, and the encrypted passwords are located in cifsPasswd in a colon-delimited text file. Normally, you do not need to change these files directly because you can do almost everything with the `net` command.

Detailed protocol-related data is saved in the /var/log/cifsLog file, which is useful for advanced troubleshooting of AIX Fast Connect.

You can check if the server is actually listening on the netbios-ssn port with the `netstat -a` command:

```
$ grep netbios /etc/services
netbios-ns      137/tcp                         # NETBIOS Name Service
netbios-ns      137/udp                         # NETBIOS Name Service
netbios-dgm     138/tcp                         # NETBIOS Datagram Service
netbios-dgm     138/udp                         # NETBIOS Datagram Service
netbios-ssn     139/tcp                         # NETBIOS Session Service
netbios-ssn     139/udp                         # NETBIOS Session Service
$ netstat -an | grep 13[7-9]
tcp4       0      0  *.139                  *.*                    LISTEN
udp4       0      0  *.137                  *.*
```

You should see the LISTEN state for netbios-ssn service (port number 139). That means that the server is running and accepting connections from the client.

A.3 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 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 a 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 status information about 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 an IP address from the computer name and vice versa.
- **arp** - This shows and modifies the table for IP addresses to adapter address translation.

Try to find out if the problem is only only one computer.

A.4 Troubleshooting utilities on Windows NT

This section describes Windows NT tools for TCP/IP and SMB diagnostics.

A.4.1 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 an 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
```

On Windows 95 systems, you can use the `winipcfg` command to get similar information.

You can use other commands to help you analyze the configuration, routing, DNS, and other TCP/IP related problems, such as hostname, ping, netstat, route, arp (see Appendix A.3, “Generic TCP/IP utilities” on page 169).

You may try using the Solving Basic TCP/IP Problems procedure on the following Web site:
`http://support.microsoft.com/support/tshoot/nt4_tcp.asp`

A.4.2 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.4.2.1 tracert commands

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 TTL value (time-to-live). 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 a loose source route along host-list.

`-w` This specifies 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.4.2.2 nbtstat tool

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` This lists the remote computer's name table (similar to what option -n does for a local computer).

`-c` This shows the content of NetBIOS name cache.

`-r` This shows the name resolution and registration statistics as well as names resolved by broadcast.

`-R` This clears the local cache and reloads it from the LMHOSTS file.

`-s, -S` This lists the NetBIOS sessions. The first option will show NetBIOS names and the second one will show 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.4.2.3 browstat utility

The *Microsoft Windows NT Server Resource Kit 4.0* includes the browstat utility, which can be used to analyze 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, `NetBF_Ibmtok51` and `Nbf_Ibmtok51`, in this example.

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 the following 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 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). 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.5 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.5.1 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.5.2 Fast Connect server troubleshooting

The following sections describe commands that may help you determine what the trouble is with your server.

A.5.2.1 The Fast Connect server net command

The command line administration program is the `net` command. This command has a syntax similar to the one you have with Windows systems. The most important options for troubleshooting are:

help [command]

This shows the list of main options or a description of an individual option of the `net` command.

status

This shows the server state (see Figure 146) and the server NetBIOS and TCP/IP name:

```
$ net status
Server lv3030c has been paused on lv3030c.itsc.austin.ibm.com.
```

statistics [/reset]

This shows statistics of the server's sessions, connections, and errors since the last server start or the last reset of the statistics (option /reset). You should be careful about resetting statistics because you could get less information from net statistics. You can solve this by doing /reset when there is no client connected to the server. You can see additional information about statistics analyzed in Appendix A.5.2.2, "net statistics command" on page 177.

user

Show and change user settings. User manipulation is only necessary when you use AIX Fast Connect authentication. Important options are:

net user [password|-p] [/add] [/active:[0|1]] /changeaixpwd:[yes|no]

Add a user with the specified password and/or (de)activate one. You cannot add a user that is not also an AIX user. If you select -p, you are prompted for the password, and the password is not displayed on the screen. Like all the other changes operated with the `net` command, only root can change the password of the user. If you want to change both the AIX and Fast Connect password at the same time, you can use the /changeaixpwd:yes option.

nbstatus

This shows the status of NBNS (running or not running).

nblistnames

This lists NetBIOS names from the NetBIOS name table.

A.5.2.2 net statistics command

You can quickly check for SMB protocol problems with the `net statistics` command. Output from this command looks like this:

```
Server lv3030c running on lv3030c.itsc.austin.ibm.com since
Fri Feb  5 11:50:21 1999

Server statistics since Fri Feb  5 11:50:21 1999

Sessions started                                8
Sessions timed out                              6
Sessions dropped                                7
Password Errors                                 7
Permission Errors                               4
Bytes sent low                                  10649
Bytes sent high                                 0
Bytes received low                              8042
Bytes received high                             0
Request buffer failures                         0
Big buffer failures                             0
Print jobs queued                               0
```

You can see the server name, server startup time, and statistics startup time in the header. Then, you can see the following values:

Sessions started — This counts the number of sessions initiated from the clients.

Sessions timed out — This counts the number of sessions that were disconnected because of inactivity time (related to the autodisconnect parameter).

Sessions dropped — This counts the number of sessions that ended - with or without error.

Password Errors — This counts the number of errors because of illegal passwords. It is not necessarily a serious matter if this number is not zero. Maybe a guest account was used or somebody simply mistyped a password. The first step is for the client to send the user's name and password, which can be rejected (thus the error), and then request guest account, which is accepted.

Permission Errors — This counts the number of file permission errors.

Print jobs queued — This counts the number of jobs submitted to printer queues.

You can continuously watch net statistics output if you enter:

```
clear; while (true); do tput home; net statistics; sleep 2; done
```

If server and statistics startup time do not match, you must be careful about interpreting the results. For example, if you reset the statistics in the middle of some sessions, all active sessions will register just at the end of the session, and you can later see more dropped (ended) sessions than started ones.

A.5.3 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.5.3.1 iptrace utility

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 only trace 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, which can then be processed with the `ipreport` command. The syntax for the iptrace utility is:

`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:

```
$ 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.5.3.2 tcpdump command

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 an interface to which to listen. 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 (for example, lv3030c instead of lv3030c.itsc.austin.ibm.com).
-q	This quiets output. Output lines contain 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 the expression is true, the packet is accepted. Expressions consists of one or more primitives. The important primitives are:

[src | dst] host host	This is true if the source or destination is a host with a specified host name. You can limit the selection to only the 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 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:

Show all traffic from/to the lv3030c computer:

host lv3030c

Show traffic from/to a machine with a specified IP address:

ip host 9.3.187.21

Show traffic from lv3030c to ausres10:

srchost lv3030c and dst host ausres10

Show NetBIOS traffic involving host lv3030c:

\(port netbios-ns or port netbios-dgm or port netbios-ssn \) and host lv3030c

Same as previous example:

\(port 137 or port 138 or port 139 \) and host lv3030c

The important ports for diagnosing the SMB protocol are:

netbios-ns (port 137) is NetBIOS Name Service.

netbios-dgm (port 138) is NetBIOS Datagram Service.

netbios-ssn (port 139) is NetBIOS Session Service.

If you want to see, say, the packet traffic between client and server, when the client runs the `net view` command, the client output will look like the following:

```
C:\>net view \\lv3030c
Shared resources at \\lv3030c

Fast Connect 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 the following command:

```
$ 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. An 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.5.3.3 trace

The trace facility helps you isolate system problems by monitoring selected system events. You must have the bos.sysmgt.trace package installed. This utility is normally used by IBM specialists. You must specify the system events (called hooks) that you want to catch. Some hooks that are interesting for analyzing TCP/IP level of networking are:

251 HKWD NETERR Records TCP/IP network error events

252 HKWD SYSC TCPIP Records socket-type system call events on entry and exit to socket-type subroutines

253 HKWD SOCKET Records TCP/IP socket layer events

25A HKWD TCPDBG Records outgoing and incoming packets on the TCP level

There are also some hooks, related to the Fast Connect server events:

- 2EE CIFS Enter
- 2EF CIFS Exit
- 2F0 CIFS-FSS
- 2F1 CIFS-Logon
- 2F2 CIFS-Net
- 2F3 CIFS-SMB Parser
- 2F4 CIFS-PSS

- 2F5 CIFS-SMS

When you want to use the trace facility, perform the following steps:

1. Enter the `trace` command where you select all appropriate hooks. If you are not sure which hooks are the right ones, select all of them as shown in the following example:

   ```
   trace -a -j 251,252,253,25A -o trace_bin_file
   ```

2. Recreate the problem with minimal possible steps.
3. Stop the trace facility with the `trcstop` command.
4. Create a trace report:
5. trcrpt *trace_bin_file* > *trace_report_file*
6. An example of a trace report looks like the following screen:

```
$ trace -a -j 2EE,2EF,2F0,2F1,2F2,2F3,2F4,2F5
.....
$ trcstop
$ trcrpt /var/adm/ras/tracefile

Thu Feb  4 11:25:51 1999
System: AIX lv3030c Node: 4
Machine: 006151444C00
Internet Address: 0903BBD5 9.3.187.213
Buffering: Kernel Heap

trace -a -j 2EE,2EF,2F0,2F1,2F2,2F3,2F4,2F5 -o /var/cifs/cifs.trace

ID     ELAPSED_SEC     DELTA_MSEC   APPL    SYSCALL KERNEL  INTERRUPT

001    0.000000000       0.000000                  TRACE ON channel 0
                                                   Thu Feb  4 11:25:51 1
2EE   39.185806317    39185.806317                 CIFS Enter LS_NBProcN
2F2   39.185907517        0.101200                 CIFS-NET data 32804 s
9.3.240.113
2F2   39.186005583        0.098066                 CIFS-NET data 32806 s
```

If you have problems with the Fast Connect server and must collect trace information for analysis, you should trace the following hooks:

```
trace -aj 2EE,2EF,2F0,2F1,2F2,2F3,2F4,2F5
...
trcstop
tar cvf trace.tar -C /var/adm/ras trcfile
```

Normally, you should also add the following information:

- Machine type
- oslevel output
- netstat -an output
- lslpp -a output
- Amount of memory
- Configuration file /etc/cifs/cifsConfig
- Log file /var/cifs/cifsLog
- Information about installed software: lslpp -l
- Error reports: errpt, errpt -a
- Listing of running processes: ps aux, ps -efl

A.6 Common problems

Here is a list of some common problems and hints with the Fast Connect server.

A.6.1 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 Windows Internet Name Service. If the Status field is Started, WINS is running on the server.
- Enable LMHOSTS for name resolution and add the 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 to check NetBIOS name resolution.

A.6.2 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.6.3 Authentication

- Check whether the guest account is enabled and whether the guest user name is appropriate for an AIX user.

A.6.4 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 whether 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 this 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:

```
delprof [/p] [/c:\\computer]
```

The flags are:

/p	Prompt before deleting profile
/c:\\computer	Specify remote computer

Enable logging of user profile actions
You can use the checked version of UserEnv.dll library, which is located on the Windows NT Device Driver Kit (DDK) or Windows NT Software Development Kit (SDK). The steps to use this library are as follows:

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

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\Winlogon
   ```

   create a new value, UserEnvDebugLevel (REG_DWORD), the with value 10002.
4. Reboot the computer.

Logging information is recorded in the C:\UserEnv.log.

A.6.5 File system shares

- Check file and directory owner and access permissions on the server.
- Check the Fast Connect umask setting on the server.

A.6.6 Printer share

- Check a direct printing from AIX print queue on the server.
- Check and compare printer definition on both server and client.
- Create a file on 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 system engineers, I/T architects, and consultants understand the capabilities of the AIX Fast Connect For Windows and OS/2 system. The information in this publication is not intended as the specification of any programming interfaces that are provided by the AIX Fast Connect For Windows and OS/2 product. See Chapter 12, “AIX and AIX Fast Connect Server for Windows and OS/2”, of the *AIX V4.3 System Management Guide: Communications and Networks*, SC23-4127, 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:

Home Director	IBM
Netfinity	OS/2
RISC System/6000	RS/6000
SP	System/390
Wizard	

The following terms are trademarks of other companies:

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.

Lotus Notes is a registered trademark of Lotus Development Corporation.

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 193.

- *AIX and Windows NT, Solutions for Interoperability*, SG24-5102
- *Understanding IBM RS/6000 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 ibm.com/redbooks for information about all the CD-ROMs offered, updates and formats.

CD-ROM Title	Collection Kit Number
System/390 Redbooks Collection	SK2T-2177
Networking and Systems Management 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

These publications are also relevant as further information sources:

- *AIX Version 4 System Management Guide: Operating System and Devices*, SC23-2525
- *AIX Version 4.3 Network Installation Management Guide and Reference*, SC23-4113
- *AIX Version 4.3 Quick Installation and Startup Guide*, SC23-4111

- *AIX Version 4.3 System Management Guide: Communications and Networks*, SC23-4127

C.4 Referenced Web sites

These Web sites are also relevant as further information sources:

- http://service.boulder.ibm.com/asd-bin/doc/en_us/winntcl2/f-feat.htm
- http://support.microsoft.com/download/support/mslfiles/vrdrupd.exe
- http://support.microsoft.com/support/tshoot/nt4_tcp.asp
- http://www.redbooks.ibm.com/portals/rs6000

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
iFOR/LS	Information for Operation Retrieval/License System
IBM	International Business Machines Corporation
IPF	Install Package Facility
IPX	Internetwork Packet eXchange
ITSO	International Technical Support Organization
LAN	Local Area Network
LANA	Local Area Network Adapter
LDAP	Lightweight Directory Access Protocol
LPP	Licensed Program Products
LPR	Line Printer
NCP	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 UNIXClient
NetBEUI	NetBIOS Extended User Interface
OEM	Original Equipment Manufacturer
PC	Personal Computer
PDC	Primary Domain Controller
PPA	Physical Point of Attachment
RFC	Request For Comments
RIP	Routing Information Protocol
RS/6000 SP	IBM RS/6000 Scalable POWERParallel Systems.
SAM	Security Accounts Manager
SANDS	Standalone NDS
SAP	Service Advertising Protocol
SAPD	SAP daemon
SCALE	Scalable NDS
SMB	Server Message Block
SMP	Symmetric Multiprocessor
SNMP	Simple Network Management Protocol
SP	Scalable POWERParallel
SPX	Sequenced Packet eXchange
TAS	TotalNET Advanced Server
TCP/IP	Transmission Control Protocol/Internet Protocol
TNAS	TotalNET Administration Suite
VMS	Virtual Memory System

WINS	Windows Internet Name Service
Windows NT	Windows New Technology

Index

Symbols

A

B

C

D

E

F

R

S

T

U

V

W

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**	SG24-5527-00 AIX Fast Connect Functions 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/

AIX Fast Connect
Functions and Sizing Guide

Install, set up, and customize an AIX Fast Connect server

Detailed overview of advanced functionality

Practical sizing guidelines for CPU, memory, and network

AIX Fast Connect for Windows and OS/2, announced with AIX 4.3.2, was IBMs first step to let PCs take advantage of the performance, scalability, and reliability of AIX. Now, Version 2.1.1 adds powerful new features, such as DFS access and Netlogon capabilities.

This IBM Redbook walks you through the installation and setup of Fast Connect on your server. It shows you how to customize this product by declaring file shares and print shares. Since security and ease of administration of the password databases on the network are two important tasks for the system administrator, this book describes which security models are available and how to set up your PC clients to communicate with the Fast Connect server. This book also provides sizing guidelines to help you select the most adequate server for your environment.

Because of its in-depth coverage of the Fast Connect product, this book is a must-read for IT specialists with the task of recommending solutions for AIX and PC interoperability and the system administrators who will implement such solutions.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

SG24-5527-00 ISBN 0738417157