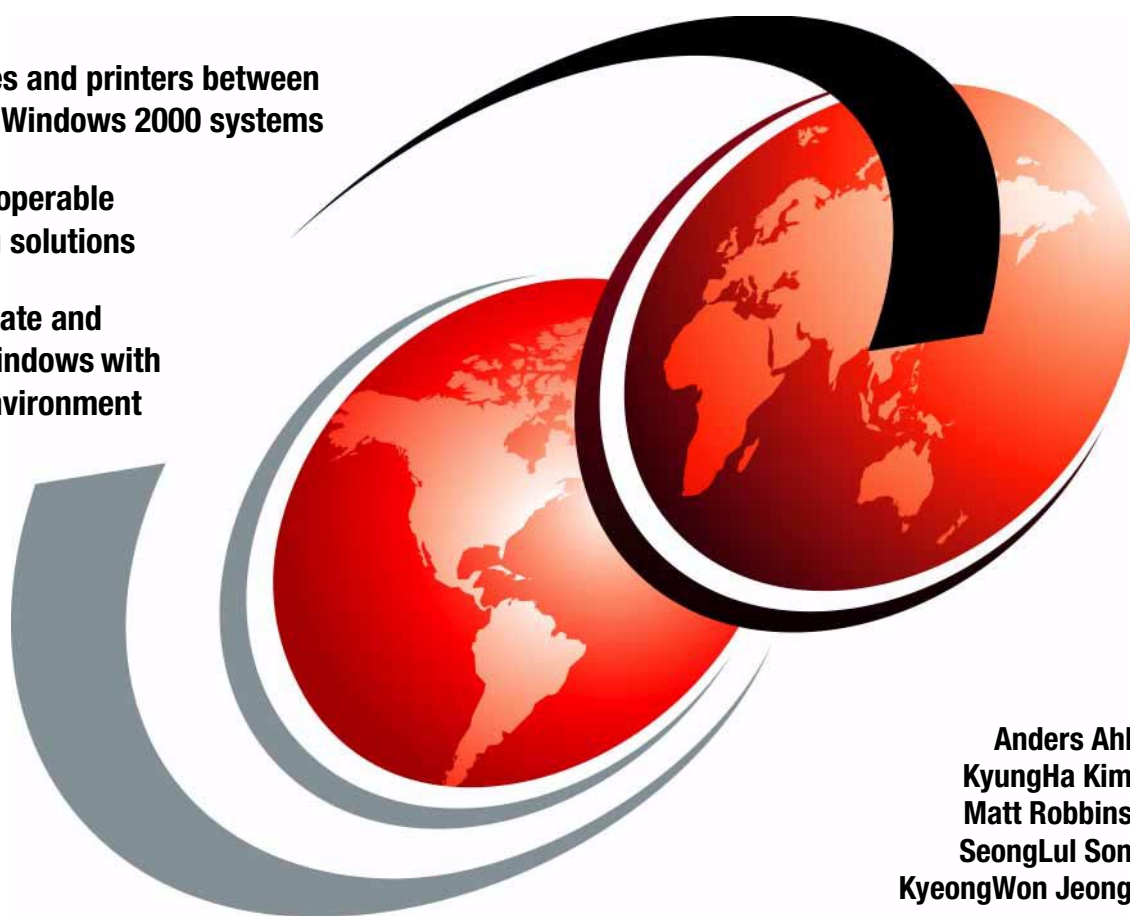


# AIX 5L and Windows 2000: Solutions for Interoperability

Sharing files and printers between AIX 5L and Windows 2000 systems

Learn interoperable networking solutions

Fully integrate and optimize Windows with your AIX environment



Anders Ahl  
KyungHa Kim  
Matt Robbins  
SeongLul Son  
KyeongWon Jeong

[ibm.com/redbooks](http://ibm.com/redbooks)

**Redbooks**





International Technical Support Organization

**AIX 5L and Windows 2000:  
Solutions for Interoperability**

May 2001

**Take Note!**

Before using this information and the product it supports, be sure to read the general information in Appendix C, "Special notices" on page 249.

**First Edition (May 2001)**

This edition applies to IBM RS/6000 systems for use with the AIX 5L Operating System Version 5.0, and is based on information available in February, 2001.

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.

**© Copyright International Business Machines Corporation 2001. All rights reserved.**

Note to U.S Government Users – Documentation related to restricted rights – Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

# Contents

<b>Figures</b> .....	vii
<b>Tables</b> .....	.xi
<b>Preface</b> .....	.xiii
The team that wrote this redbook .....	.xiii
Comments welcome .....	.xv
<b>Chapter 1. Introduction</b> .....	1
1.1 Overview .....	1
1.2 Functions .....	2
1.2.1 Solutions from basic operating systems .....	2
1.2.2 PC connectivity .....	3
1.2.3 Services for UNIX .....	4
1.2.4 Terminal emulation .....	4
<b>Chapter 2. Solutions from basic operating systems</b> .....	7
2.1 File transfer using FTP .....	7
2.1.1 FTP connection to Windows 2000 Server or Professional .....	7
2.1.2 FTP connection to AIX 5L .....	14
2.2 Printing solutions .....	16
2.2.1 Using a remote printer attached to Windows 2000 .....	16
2.2.2 Using a remote printer attached to AIX 5L .....	19
2.2.3 Using Web printing in Windows 2000 .....	22
2.3 Using Telnet .....	27
2.3.1 Remote connection to AIX 5L machine .....	27
2.3.2 Remote connection to Windows 2000 machine .....	28
<b>Chapter 3. PC connectivity solutions</b> .....	29
3.1 AIX Fast Connect .....	29
3.1.1 Overview .....	29
3.1.2 AIX Fast Connect configuration and administration .....	36
3.1.3 Accessing AIX Fast Connect Server from Windows 2000 .....	41
3.1.4 AIX Fast Connect problem determination .....	49
3.1.5 Migrating to AIX Fast Connect from AIX Connections .....	53
3.1.6 Performance considerations .....	54
3.1.7 Limitations .....	55
3.2 Samba .....	56
3.2.1 Overview .....	56
3.2.2 NetBIOS and SMB overview .....	57
3.2.3 Obtaining Samba .....	58

3.2.4	Samba support	59
3.2.5	Quick installation	59
3.2.6	Configuring the Samba daemons	61
3.2.7	Basic configuration using SWAT	62
3.2.8	Samba configuration file	72
3.2.9	Verifying Samba is installed correctly	74
3.2.10	Checking your server	75
3.2.11	Accessing the share resources from the client	76
3.2.12	Accessing resources from the Samba server	82
3.2.13	Using Samba to back up a client	86
3.2.14	Security issues	91
3.2.15	Using a remote machine to make the authentication	96
3.2.16	Joining an Windows 2000 domain for security authentication	96
3.2.17	Windows 2000 to AIX users mapping	99
3.2.18	Windows Internet Name Service (WINS)	100
3.2.19	Browsing	102
3.2.20	Troubleshooting	103
3.3	FacetWin	105
3.3.1	Overview	106
3.3.2	Installing the FacetWin AIX Server	108
3.3.3	Accessing FacetWin server from Windows 2000	114
3.3.4	Installing FacetWin on a PC	116
3.3.5	File sharing	120
3.3.6	Print sharing	121
3.3.7	FacetWin UNIX commands	123
<b>Chapter 4. Services for UNIX Version 2.0</b>		<b>127</b>
4.1	System requirements	127
4.2	Component summary	129
4.3	Installation and customization	130
4.3.1	Command line installation	130
4.3.2	GUI installation	133
4.3.3	GUI uninstallation and modification	136
4.4	User and Security components	137
4.4.1	User name mapping server	137
4.4.2	Password synchronization	141
4.4.3	Server for NIS	149
4.4.4	NIS to AD Migration Wizard	150
4.5	File system components	151
4.5.1	Client for NFS	151
4.5.2	Gateway for NFS	164
4.5.3	Server for NFS	168
4.5.4	Server for PCNFS	170

4.6	Telnet components . . . . .	170
4.6.1	Telnet server . . . . .	171
4.6.2	Telnet client . . . . .	176
4.7	Shells and utilities . . . . .	178
4.7.1	Korn shell . . . . .	178
4.7.2	UNIX utilities. . . . .	178
4.7.3	ActiveState ActivePerl 5.6 . . . . .	178
4.8	System administration . . . . .	179
4.8.1	Microsoft Management Console (MMC) . . . . .	179
4.9	Windows Management Instrumentation (WMI) . . . . .	181
<b>Chapter 5. Terminal emulation solutions . . . . .</b>		<b>183</b>
5.1	X Window Display Manager (XDM) . . . . .	183
5.2	Hummingbird Exceed . . . . .	183
5.2.1	Exceed installation . . . . .	184
5.2.2	Exceed setup . . . . .	187
5.3	Network Computing Devices PC-Xware . . . . .	191
5.3.1	PC-Xware installation . . . . .	192
5.3.2	PC-Xware configuration . . . . .	195
5.4	WRQ's Reflection . . . . .	198
5.5	Using XDM client software for interoperability solutions . . . . .	200
5.5.1	Exceed functionality . . . . .	200
5.5.2	PC-Xware functionality . . . . .	202
5.5.3	Reflection functionality . . . . .	203
5.5.4	Full X Window export to Windows desktop . . . . .	204
5.6	Citrix MetaFrame . . . . .	207
5.6.1	Overview . . . . .	207
5.6.2	MetaFrame for AIX . . . . .	210
5.6.3	MetaFrame for Windows 2000 . . . . .	221
5.6.4	Example: Running IE5 from an AIX session . . . . .	231
<b>Appendix A. SFU UNIX utilities . . . . .</b>		<b>243</b>
<b>Appendix B. From 0 to NIS in 10 easy steps . . . . .</b>		<b>247</b>
<b>Appendix C. Special notices . . . . .</b>		<b>249</b>
<b>Appendix D. Related publications . . . . .</b>		<b>253</b>
D.1	IBM Redbooks collections . . . . .	253
D.2	Referenced Web sites . . . . .	253
<b>How to get IBM Redbooks . . . . .</b>		<b>255</b>
IBM Redbooks fax order form . . . . .		256

<b>Abbreviations and acronyms</b> .....	257
<b>Index</b> .....	259
<b>IBM Redbooks review</b> .....	265



## Figures

1.	The structure of this redbook . . . . .	1
2.	Solutions from basic OS . . . . .	2
3.	PC connectivity . . . . .	3
4.	Services for UNIX . . . . .	4
5.	Terminal emulation . . . . .	5
6.	Windows 2000 desktop . . . . .	8
7.	Internet Information Services . . . . .	9
8.	Home directory configuration . . . . .	10
9.	Virtual directory creation wizard . . . . .	11
10.	Virtual directory alias . . . . .	12
11.	FTP site content directory . . . . .	13
12.	Access permission . . . . .	13
13.	TCP/IP Print Server . . . . .	17
14.	TCP/IP Print Server properties . . . . .	18
15.	Control panel - Printers . . . . .	20
16.	Add Printer Wizard . . . . .	20
17.	Select the LPR port . . . . .	21
18.	Add LPR compatible printer . . . . .	22
19.	Locating printers via Web browser . . . . .	23
20.	Printer management via Web browser . . . . .	24
21.	Printer driver installation in Web browser . . . . .	25
22.	User authentication for installing a printer driver . . . . .	26
23.	The final panel for installation of printer driver . . . . .	27
24.	AIX Fast Connect server and supported clients . . . . .	30
25.	Example of AIX Fast Connect configuration and system environments . . . . .	37
26.	Starting AIX Fast Connect server using Web-based System Manager . . . . .	38
27.	Windows 2000 Local Area Connection Properties . . . . .	42
28.	Identification changes . . . . .	43
29.	Browsing Workgroup . . . . .	44
30.	Search Results - Computers . . . . .	45
31.	AIX Fast Connect shared resources . . . . .	47
32.	Map Network Drive . . . . .	48
33.	Enter Network Password . . . . .	63
34.	SWAT start page . . . . .	64
35.	Global section in SWAT . . . . .	65
36.	Shares section in SWAT . . . . .	67
37.	Printers section in SWAT . . . . .	68
38.	Selecting printer . . . . .	68
39.	Printer properties . . . . .	69
40.	Status section in SWAT . . . . .	70

41.	View section in SWAT . . . . .	71
42.	Password section in SWAT . . . . .	72
43.	Identification Changes . . . . .	77
44.	Local Area Connection status . . . . .	78
45.	Internet Protocol (TCP/IP) Properties . . . . .	79
46.	Advanced TCP/IP Settings . . . . .	80
47.	Search for computers . . . . .	81
48.	Samba shared resources . . . . .	83
49.	Map Network Drive . . . . .	83
50.	Add Printer Wizard . . . . .	86
51.	Sharing a directory . . . . .	88
52.	Request for authentication panel. . . . .	92
53.	Password section . . . . .	94
54.	Example of using Domain security level . . . . .	98
55.	Configuration of Samba server . . . . .	99
56.	Getting the name of Workgroup/Domain. . . . .	111
57.	Locating FacetWin server . . . . .	115
58.	Accessing file shares on FacetWin server. . . . .	115
59.	Installing FacetWin on a client from a server. . . . .	116
60.	Select Components . . . . .	117
61.	FacetWin Administrator . . . . .	118
62.	FacetWin Agent Control Panel . . . . .	119
63.	File Sharing tab . . . . .	120
64.	Properties of UNIX file share . . . . .	121
65.	Properties of UNIX print shared with PCs . . . . .	122
66.	Add Printer Wizard . . . . .	123
67.	SFU - Installation options . . . . .	133
68.	SFU - Selecting components. . . . .	135
69.	SFU - Conflicting components. . . . .	136
70.	SFU - Maintenance Wizard . . . . .	137
71.	SFU - User Name Mapping . . . . .	138
72.	SFU - Simple user mapping . . . . .	139
73.	SFU - Advanced user mapping . . . . .	140
74.	SFU - Group mapping . . . . .	141
75.	SFU - Default password synchronization . . . . .	145
76.	SFU - Updated 3DES source library on Microsoft download. . . . .	146
77.	SFU - Advanced password synchronization . . . . .	147
78.	SFU - Advanced individual password synchronization . . . . .	148
79.	SFU - UNIX properties for users in AD . . . . .	150
80.	SFU - NFS Network browsing . . . . .	156
81.	SFU - Default LAN registry values. . . . .	157
82.	SFU - Add hosts to Favorite LAN . . . . .	157
83.	SFU - Custom groups in NFS Network . . . . .	159

84.	SFU - Add/Remove NFS LANs . . . . .	159
85.	SFU - Add Broadcast LAN . . . . .	160
86.	SFU - Added a new dynamic NFS group . . . . .	160
87.	SFU - Server export properties . . . . .	161
88.	SFU - Client for NFS default file access permissions . . . . .	162
89.	SFU - Client for NFS performance settings. . . . .	163
90.	SFU - Gateway for NFS Shares . . . . .	165
91.	SFU - NFS Attributes tab. . . . .	166
92.	SFU - NFS Mount Options tab . . . . .	167
93.	SFU - NFS Sharing tab . . . . .	168
94.	SFU - Server for NFS logging . . . . .	169
95.	SFU - Server for NFS locking . . . . .	170
96.	SFU - Telnet Server Authentication options . . . . .	171
97.	SFU - Telnet Server Event log entry . . . . .	172
98.	SFU - Telnet Server Logging options . . . . .	173
99.	SFU - Telnet Server Settings . . . . .	174
100.	SFU - Telnet Server Sessions . . . . .	175
101.	MMC user interface elements . . . . .	180
102.	SFU - Servers and clients console . . . . .	181
103.	Exceed user name and security options . . . . .	184
104.	Exceed choose installation type . . . . .	185
105.	Exceed set password for Xconfig . . . . .	186
106.	Exceed tune Xserver graphics settings. . . . .	187
107.	Exceed starting Xconfig. . . . .	188
108.	Exceed configure XDM . . . . .	188
109.	Exceed specify IP for XDM query . . . . .	189
110.	Exceed restart server for XDM . . . . .	189
111.	Exceed start XDM client . . . . .	190
112.	Exceed XDM broadcast panel. . . . .	191
113.	PC-Xware archive extraction. . . . .	192
114.	PC-Xware installation type . . . . .	193
115.	PC-Xware registration information. . . . .	194
116.	PC-Xware installation path . . . . .	194
117.	PC-Xware configure XDM session . . . . .	195
118.	PC-Xware specify XDM type . . . . .	196
119.	PC-Xware specify IP address . . . . .	197
120.	PC-Xware specify name for icon . . . . .	198
121.	Reflection X startup panel . . . . .	199
122.	Reflection xterm startup panel. . . . .	200
123.	Exceed toolbat. . . . .	201
124.	Exceed xterm exported to Windows desktop . . . . .	202
125.	PC-Xware xterm session exported to Windows desktop. . . . .	203
126.	Reflection export an xterm session . . . . .	204

127. CDE and Windows 2000 working together . . . . .	205
128. Cutting and pasting between X Windows and Windows applications . .	206
129. User interface transportation over ICA . . . . .	208
130. ICA bandwidth consumption . . . . .	208
131. MetaFrame Win2K - Network ICA connections . . . . .	222
132. Citrix Connection Configuration . . . . .	224
133. Edit Connection . . . . .	225
134. Advanced Connection Settings . . . . .	226
135. Client Settings . . . . .	227
136. ICA browser configuration . . . . .	228
137. ICA client database . . . . .	229
138. ICA Client name . . . . .	231
139. Enter Application Name . . . . .	232
140. Define the Application . . . . .	233
141. Select Domain or Citrix Server . . . . .	234
142. Configure Accounts . . . . .	235
143. IE5 successfully published . . . . .	236
144. Empty AIX ICA client . . . . .	236
145. Network properties . . . . .	237
146. Connection Selection . . . . .	238
147. Window properties . . . . .	239
148. IE5 defined as an ICA application . . . . .	240
149. IE5 running seamless in CDE . . . . .	241

## **Tables**

1. Other server software with known conflicts . . . . .	32
2. AIX Fast Connect packaging . . . . .	33
3. AIX Fast Connect files . . . . .	34
4. AIX Fast Connect default parameter values . . . . .	35
5. AIX Fast Connect trace hooks . . . . .	51
6. AIX Connection configuration files . . . . .	53
7. NetBIOS/ix configuration files . . . . .	53
8. Search cache parameters . . . . .	54
9. TCP/IP ports used by NetBIOS over TCP/IP . . . . .	58
10. Parameters in the Global section . . . . .	66
11. Share parameters . . . . .	73
12. Printing parameters . . . . .	74
13. Security mode in Samba server . . . . .	91
14. Microsoft Services for UNIX Version 2.0 component availability . . . . .	127
15. msixexec.exe command line options and parameters . . . . .	131
16. Installed components in Standard installation . . . . .	134
17. SFU 2.0 UNIX utilities . . . . .	243



## **Preface**

This redbook is intended to help you understand how to integrate and optimize your AIX systems into a Windows 2000 environment, and share AIX resources with your Windows 2000 machines. We have focused our descriptions on the key areas of file and printer sharing.

This redbook will discuss the various connectivity solutions available for AIX 5L so it can inoperate with Windows 2000 machines. Solutions that will be covered for solutions for interoperability include:

- AIX Fast Connect
- Samba
- FacetWin
- Services for UNIX
- Exceed
- PC-Xware
- Reflection
- MetaFrame

These products were chosen because of their popularity with customers and their availability from IBM.

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

---

### **The team that wrote this redbook**

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

**KyeongWon Jeong** is a Senior I/T Specialist at the International Technical Support Organization, Austin Center. He writes extensively on AIX and creates education materials. Before joining the ITSO, he worked in IBM Global Learning Services in Korea as a Senior Education Specialist, and was a class manager for all AIX classes for customers and interns. He has many years of teaching and development experience.

**Anders Ahl** is an Advisory I/T Specialist for IBM Global Services in Sweden. He is Tivoli IT Director Certified and an MCSE with over nine years of experience in the Windows NT/2000 fields. His areas of expertise include IBM @server xSeries systems management, Citrix Metaframe, and TCP/IP communication.

**KyungHa Kim** is an Advisory I/T Specialist who has worked for IBM Korea since June 1996. Her areas of expertise include providing technical support on the AIX platform. Her mission includes various @server pSeries benchmark tests, performance tuning, troubleshooting, and ISV support. She holds a degree in Mathematics.

**Matt Robbins** is an @server pSeries Technical Sales Specialist in Dallas, Texas. He has over six years of experience working with pSeries systems and AIX. His areas of expertise include UNIX, TCP/IP, and designing e-business solutions for Internet security and Web traffic. He attended the University of North Texas as a student of computer science.

**SeongLul Son** is an Advisory Education Specialist in IBM Korea. He is an MCSE and CCNA with five years of experience in Microsoft Operating Systems and the AIX field. His areas of expertise include Windows NT/2000, UNIX, TCP/IP, and Internetworking between different operating systems and network devices.

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

**International Technical Support Organization, Austin**

Ella Buslovich, Ernest A. Keenan, Scott Vetter, Wade Wallace

**IBM Austin**

Linda Disney, Prasad Potluri

**IBM Sweden**

Mikael Nordström

**FacetCorp.**

Tre Groeschel, Paul Vance

**Hummingbird Ltd.**

Rana Aluraibi, Ray Wylie

**Citrix UK**

Chrystèle Bruel, Jon Rolls



**Sweden**  
Patrik Moberg

**We would also like to thank the authors of the previous “AIX and Windows NT Solutions for Interoperability” publication:**  
Zoran Gagic, Laurent Vanel, Borut Znidar

---

## **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 265 to the fax number shown on the form.
- Use the online evaluation form found at [ibm.com/redbooks](http://ibm.com/redbooks)
- Send your comments in an Internet note to [redbook@us.ibm.com](mailto:redbook@us.ibm.com)



## Chapter 1. Introduction

Many environments have a mixture of AIX-based servers and clients and Windows-based servers and clients. There are many issues associated with administering a mixed environment that enables users to share resources between both AIX and Windows 2000 clients and work efficiently with all servers and clients.

In this chapter, we will give a brief map of this redbook. You can see what kind of solutions we have, and how they can be used in various environments.

---

### 1.1 Overview

It is not the intention of this publication to cover the installation of AIX and Windows 2000, or to demonstrate how to configure TCP/IP on these systems. Figure 1 describes the structure of this redbook.

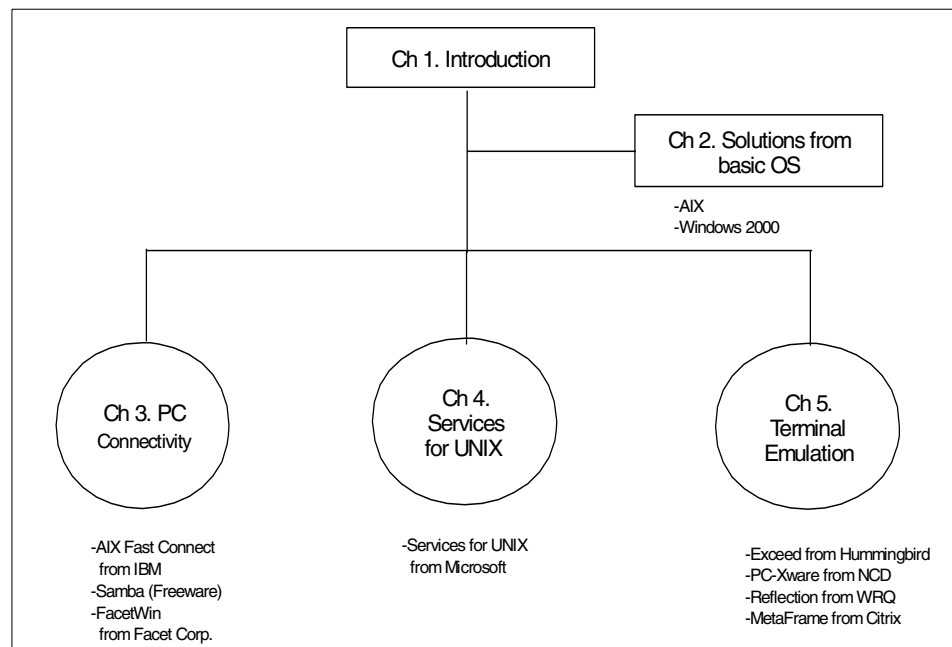


Figure 1. The structure of this redbook

As you see Figure 1, we will introduce several solutions in each area. We are not going to say that these specific solutions are always the best or one is

better than the others; there are many more solutions in the real world. Choose one or more solutions, depending on your environment and business requirements.

---

## 1.2 Functions

In this section, we will cover the functions of each product to give a general idea of each and help you compare them.

### 1.2.1 Solutions from basic operating systems

For interoperability between AIX 5L and Windows 2000, you can use features in the operating system itself. It basically provides file and print sharing service. Figure 2 summarizes this function.

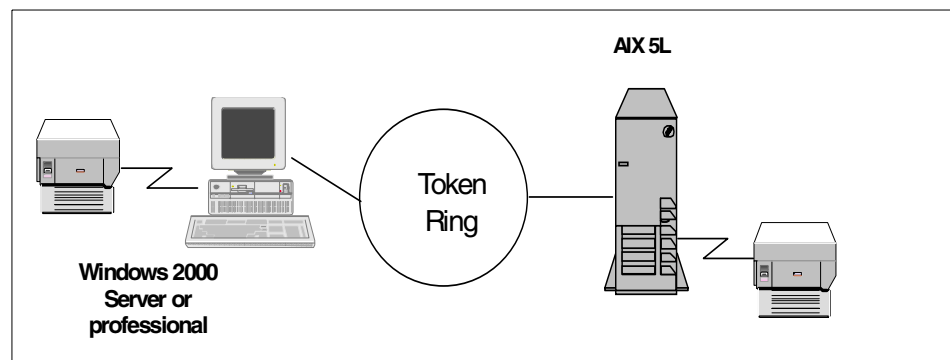


Figure 2. Solutions from basic OS

- As a FTP server, Windows 2000 can provide the file service to AIX 5L clients.
- As a FTP server, AIX 5L can provide the file service to Windows 2000 clients.
- As a print server, Windows 2000 can provide the print service to AIX 5L clients.
- As a print server, AIX 5L can provide the print service to Windows 2000 clients.

This type of solution is very useful if you do not want to install any software outside of the operating system. However, some users may find it difficult to get file service with this solution because they are not familiar with FTP commands. This solution, on the other hand, is all free. All you need to is install some services from your operating system CDs.

For more detailed information, refer to Chapter 2, “Solutions from basic operating systems” on page 7.

### 1.2.2 PC connectivity

In this section, we have three solutions; AIX Fast Connect, Samba, and FacetWin. We summarize the function of these products, which is shown in Figure 3.

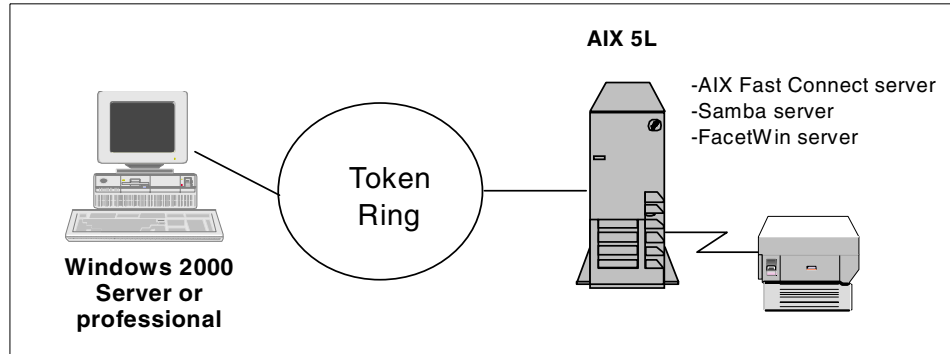


Figure 3. PC connectivity

- As a file server (SMB server), AIX 5L can provide the file service to Windows 2000 clients.
- As a print server (SMB server), AIX 5L can provide the print service to Windows 2000 clients.

One benefit of using these three products is that a client can connect to a file or print share on AIX 5L in the exact same way you connect to a Windows file or print share. In other words, the file and printer shares that you define on the AIX system appear in the PC's My Network Places just like any other Windows network resource share. It is totally transparent to the clients, so they do not have to know other commands, such as FTP.

You have to pay for using AIX Fast Connect and FacetWin, although the trial version of AIX Fast Connect server is in the bonus pack of AIX CDs, and you can download the FacetWin evaluation package from their Web site:

[http://www.facetcorp.com/fw\\_download.html](http://www.facetcorp.com/fw_download.html)

Samba is freeware and provides good functionality. However, no company has ownership of this product, which means there is no guarantee of function or technical support.

For more detailed information, refer to Chapter 3, “PC connectivity solutions” on page 29.

### 1.2.3 Services for UNIX

Microsoft developed Services for UNIX to integrate the Windows environment with UNIX. Some of the features of Services for UNIX are seen in Figure 4.

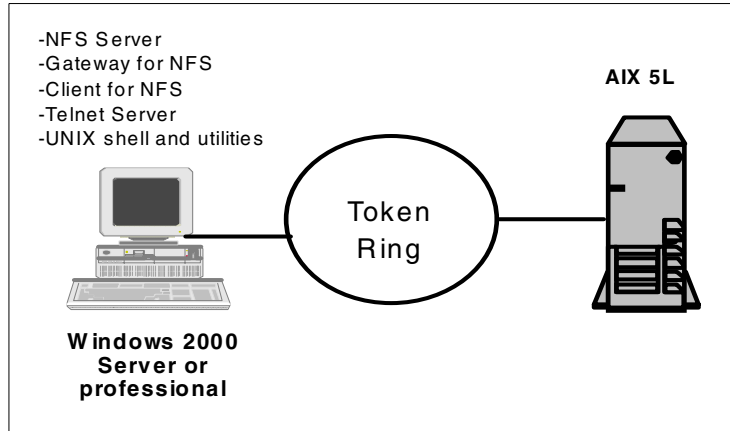


Figure 4. Services for UNIX

- As a NFS server, Windows 2000 can provide the file service to AIX 5L NFS clients.
- As a NFS client, Windows 2000 can mount file systems from an AIX 5L NFS server.
- As a gateway for NFS server, Windows 2000 Server can provide NFS service to Windows clients.
- As a telnet server, Windows 2000 allows AIX 5L users to login remotely.

Services for UNIX is not on the basic operating system CD; it must be ordered separately.

For more detail information, refer to Chapter 4, “Services for UNIX Version 2.0” on page 127.

### 1.2.4 Terminal emulation

The most popular program for terminal emulation is telnet. But sometimes you want to have an AIX 5L graphical user interface on a Windows 2000 desktop, or a Windows 2000 graphical user interface on your AIX 5L desktop.

In Chapter 5, “Terminal emulation solutions” on page 183, we will introduce four products that will allow terminal emulation: Exceed, PC-Xware, Reflection, and MetaFrame.

We will summarize the functionalities of these products, as shown in Figure 5.

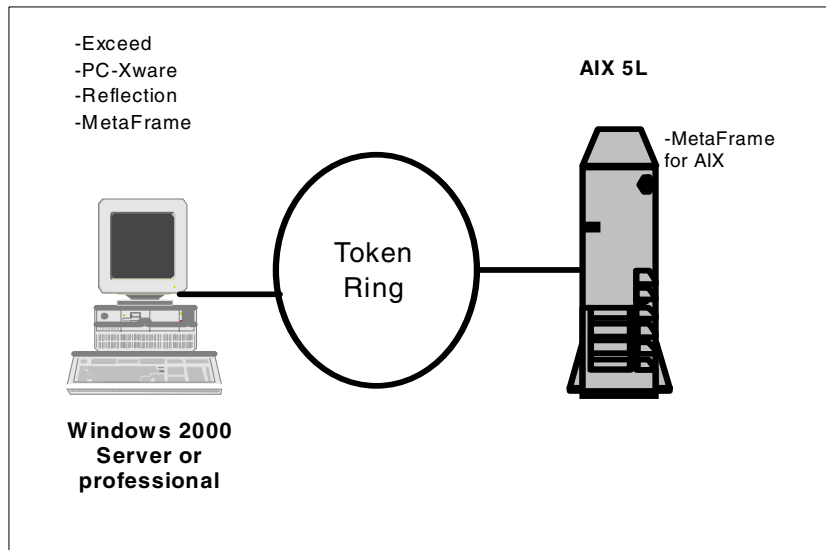


Figure 5. Terminal emulation

With Exceed, PC-Xware, and Reflection, you can have an AIX 5L GUI on your Windows 2000 or Microsoft Windows operating system.

With MetaFrame, you can have a AIX 5L GUI on your Windows 2000 operating system, and a Windows 2000 GUI on your AIX 5L operating system.

For more detailed information, refer to Chapter 5, “Terminal emulation solutions” on page 183.





---

## Chapter 2. Solutions from basic operating systems

In the case of very limited AIX 5L and Windows 2000 interoperability, such as occasional file transfers, special print jobs on specific printers, or a remote connection to manage the AIX 5L server, you can find some solutions in the basic AIX 5L and Windows 2000 operating systems. The advantage of this, of course, is that you do not need to pay extra money to use this solution, and it might be the simplest way you can find.

In this chapter, we mainly discuss file and print sharing service from both AIX 5L and Windows 2000, and some remote access services.

---

### 2.1 File transfer using FTP

To transfer files between AIX 5L and Windows 2000, the `ftp` command is the simplest answer. This client is available on both AIX 5L and Windows 2000. Note that the FTP server is not installed in Windows 2000 by default. Therefore, if you are using AIX 5L and want to connect to Windows 2000 as a FTP client, you will need to install the FTP server in Windows 2000.

#### 2.1.1 FTP connection to Windows 2000 Server or Professional

When you install Windows 2000 Server or Professional, the FTP server is not installed by default. You can perform the following steps to install FTP server on Windows 2000:

1. Locate the FTP server service and select these items in the following order:  
**Start -> Settings->Control Panel -> Add/Remove Programs -> Add/Remove Windows Components -> Internet Information Services -> details -> File Transfer Protocol (FTP) Server**
2. Choose **FTP server service** and then click **OK**.
3. Click the **Next** button. You will need a Windows 2000 CD unless you have one on your local hard disk.

#### Note

When FTP server is installed in Windows 2000, you can access it using `ftp` from AIX 5L. However, unlike AIX 5L, you must copy all the files you wish to access on Windows 2000 into the FTP home directory or configure virtual directories for AIX 5L users to use.

For initial configuration, perform the following steps:

1. Select **Internet Information Services** by *right-clicking* **My computer** -> **Manage**, as shown in Figure 6.

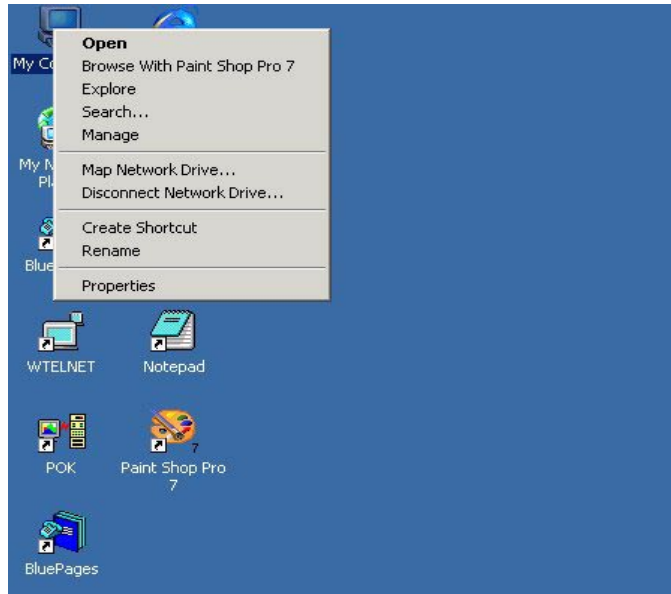


Figure 6. Windows 2000 desktop

2. Expand **Services and Applications** -> **Internet Information Services** and right-click **Default FTP Site**, as shown in Figure 7 on page 9.

**Note**

You might have a slight different look with Windows 2000 Server, as we used Windows 2000 Professional in this test environment. But the basic functions will be the same.

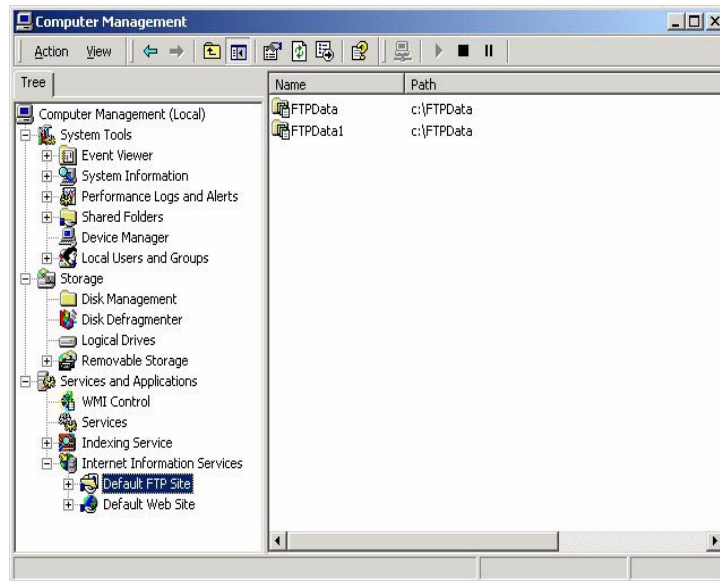


Figure 7. Internet Information Services

3. Click **Properties** and select the **Home Directory** tab.

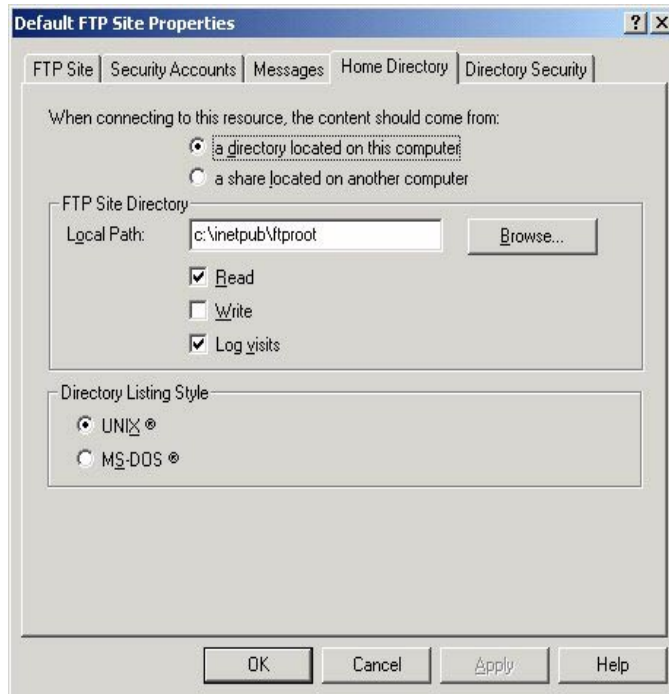


Figure 8. Home directory configuration

As you can see in Figure 8, the default directory for the FTP server is `c:\inetpub\ftproot`, assuming that you installed Windows 2000 in the C: drive. In the Home Directory tab, you can change the following configurations:

- Specify where the FTP content is stored, either locally or on another server
- Configure the default parent directory for the FTP service
- Choose the directory listing style for the FTP site
- Configure the access permissions for the FTP root directory

The initial default configuration for this directory is read-only with logging configured. However, there might be times when you want to designate a subdirectory so that clients can upload files. In this case, select both read and write for that subdirectory only.

Sometimes you do not want to copy all the files into the FTP server home directory. This is a time-consuming task, and you have to waste a lot of disk

space to have the same files in two different places. In this kind of situation, a virtual directory is a good solution.

To configure a virtual directory, select **Internet Information Service** and right-click **Default FTP Site** -> **New** -> **Virtual Directory**, as shown in Figure 9.



Figure 9. Virtual directory creation wizard

Click **Next** and type the alias you want to use to gain access to this virtual directory, as shown in Figure 10.

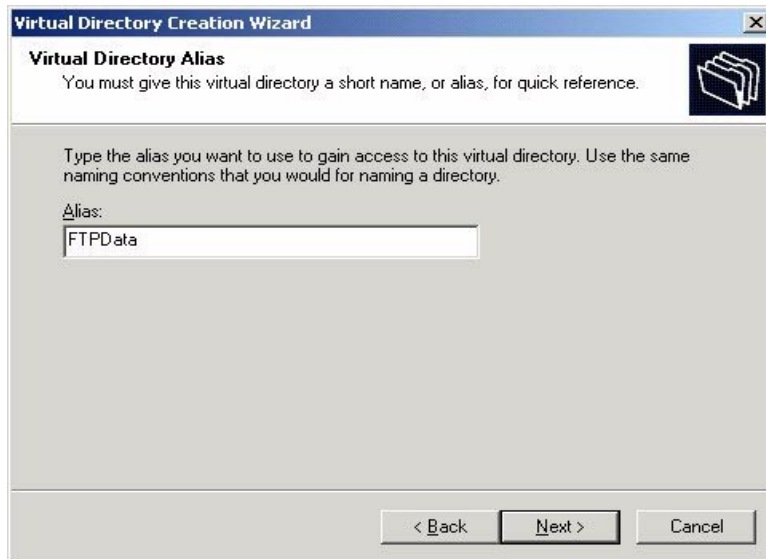


Figure 10. Virtual directory alias

Enter the path to the folder physically containing the content, as shown in Figure 11 on page 13.

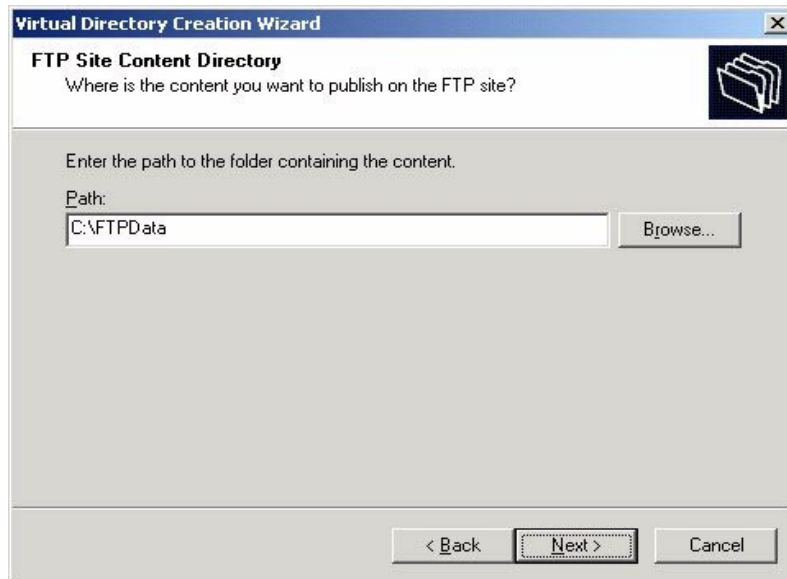


Figure 11. FTP site content directory

Choose read, write, or both for access permission based on your business requirements, select **Next**, and finally click **Finish**, as shown in Figure 12.

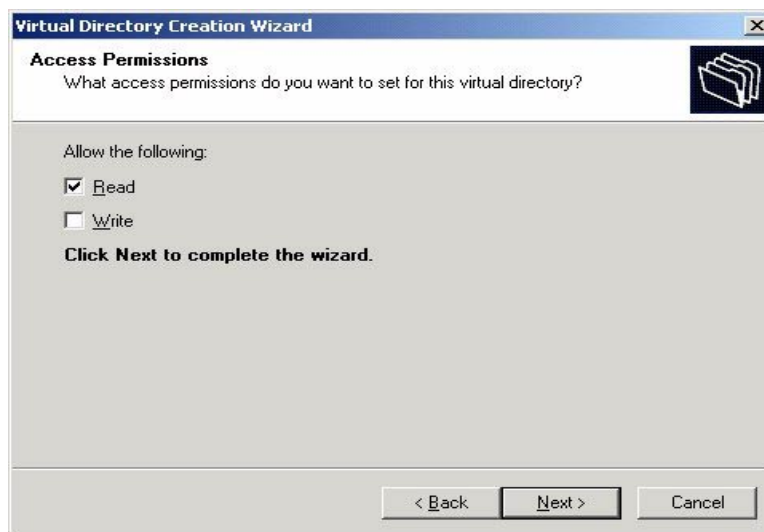


Figure 12. Access permission

Now the users in AIX 5L can access the Windows 2000 FTP server using FTP commands.

**Note**

The users in AIX 5L can access the FTP directory with the alias name only, so they should be provided with the correct alias for each directory.

The following screen is an example of an FTP connection from AIX 5L to Windows 2000.

```
# ftp w2kpro
Connected to w2kpro.
220 w2kpro Microsoft FTP Service (Version 5.0).
Name (w2kpro:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 Anonymous user logged in.
ftp> cd ftpdata
250 CWD command successful.
ftp> ls -l
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
dr-xr-xr-x  1 owner  group           0 Feb  5 15:54 Adobe
dr-xr-xr-x  1 owner  group           0 Feb  5 16:16 graphics
-r-xr-xr-x  1 owner  group       822 May 21  1999 IBMLU.txt
226 Transfer complete.
ftp>
```

### 2.1.2 FTP connection to AIX 5L

Transferring files to AIX 5L using FTP is very simple and popular. You do not need to install any software for this connection. That is why many people use FTP for file transfer between AIX 5L and Windows 2000. FTP can be used interactively. Refer to the screen below to see which FTP commands you can use in Windows 2000.



```

C:\>ftp
ftp> ?
Commands may be abbreviated.  Commands are:

!           delete          literal          prompt          send
?           debug            ls              put             status
append     dir              mdelete        pwd             trace
ascii     disconnect      mdir           quit            type
bell      get             mget          quote           user
binary    glob            mkdir          recv           verbose
bye      hash            mls           remotehelp
cd       help            mput          rename
close   lcd             open          rmdir
ftp>

```

This command is available only if the TCP/IP protocol has been installed. FTP is a service that, once started, creates a sub-environment in which you can use `ftp` commands, and from which you can return to the Windows 2000 command prompt by typing the quit subcommand. When the `ftp` sub-environment is running, it is indicated by the `ftp` command prompt.

The screen below is a typical use of FTP connection to AIX 5L from Windows 2000.

```

C:\>ftp 9.3.240.67
Connected to 9.3.240.67.
220 rs9916d FTP server (Version 4.1 Fri Sep 22 01:01:42 CDT 2000) ready.
User (9.3.240.67:(none)): slson
331 Password required for slson.
Password:
230 User slson logged in.
ftp> cd /tmp/graphics
250 CWD command successful.
ftp> ls -l
200 PORT command successful.
150 Opening data connection for /bin/ls.
total 80
-rw-r--r--  1 root    system      38097 Feb 05 16:00 graphic1.gif
226 Transfer complete.
ftp: 81 bytes received in 0.01Seconds 8.10Kbytes/sec.
ftp> bin
200 Type set to I.
ftp> get graphic1.gif ./graphic1.gif
200 PORT command successful.
150 Opening data connection for graphic1.gif (38097 bytes).
226 Transfer complete.
ftp: 38097 bytes received in 0.03Seconds 1269.90Kbytes/sec.
ftp>

```

---

## 2.2 Printing solutions

Another remote resource you can use between the two operating systems is a printer. Our solution for using a printer remotely is to use the `lpr` and `lpd` commands. Let us see how to configure your systems to do that.

### 2.2.1 Using a remote printer attached to Windows 2000

For AIX 5L users who want to use a remote printer attached to Windows 2000 Server or Professional, you need to install a service called *Print Services for Unix* in the control panel. Install this service as follows:

Select **Start -> Settings -> Control Panel -> Add/Remove Programs -> Add/Remove Windows Components -> Other Network File and Print Services -> Print Services for Unix.**

or

1. Right click on **My Network Places**, then click **Properties**.
2. In the **Advanced** menu, select **Other Network File and Print Services -> Print Services for Unix.**

**Note**

The Windows 2000 CD will be needed for this installation.

Once you have Print Services for Unix in your Windows 2000 Server or Professional, the printer attached to the Windows 2000 machine can either be a printer server or client for UNIX.

To make sure your Print Services for Unix is successfully installed, check out the list of Services currently running on your machine. The name of this service is TCP/IP Print Server.

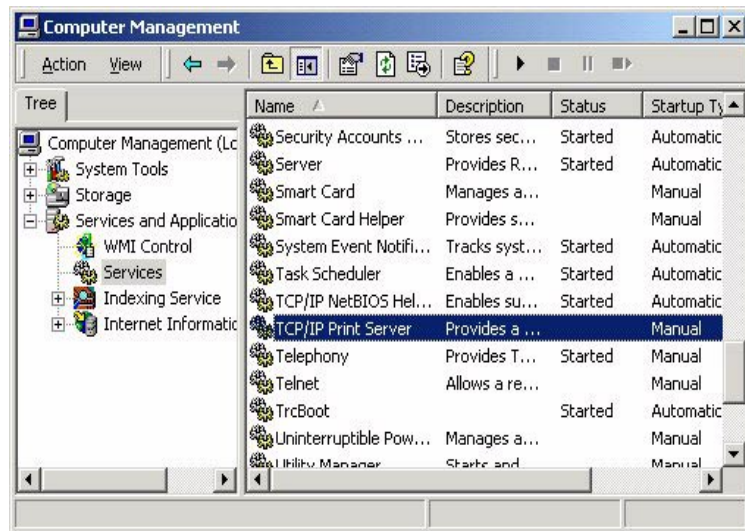


Figure 13. TCP/IP Print Server

If TCP/IP Print Server service is in the list and started, as shown in Figure 13, you can print from AIX 5L to a printer attached in Windows 2000. You may want to change *Startup Type* from *Manual* to *Automatic* so that this service will automatically start when you boot your Windows 2000 machine. Simply double click on TCP/IP Print Server and change Manual to Automatic as shown in Figure 14 on page 18. If it remains Manual, you need to manually start every time you boot the machine.

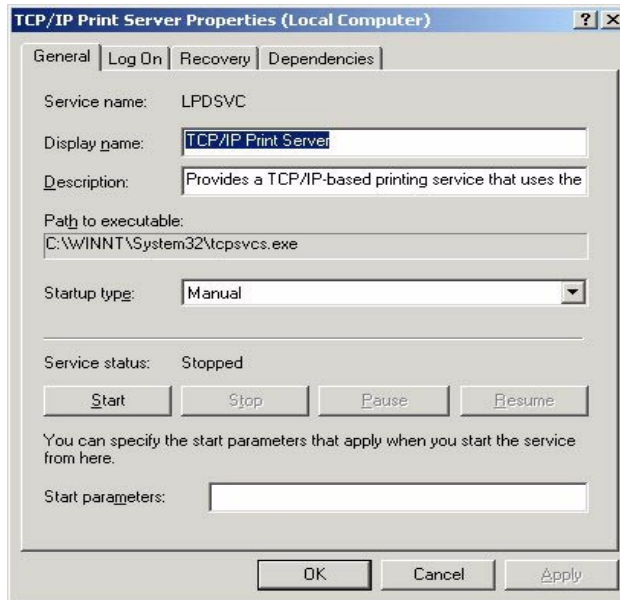


Figure 14. TCP/IP Print Server properties

Assuming that you have a printer (the Share or Queue name is w2kprint in this example) on a Windows 2000 machine and you want to print from AIX 5L, then you need to add a remote print queue in AIX machine, as seen in the following screen.

Add a Standard Remote Print Queue

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

		[Entry Fields]	
*	Name of QUEUE to add	[w2kprint]	
*	HOSTNAME of remote server	[9.3.1.180]	
*	Name of QUEUE on remote server	[w2kprint]	
	Type of print spooler on remote server	AIX Version 3 or 4	+
	Backend TIME OUT period (minutes)	[ ]	#
	Send control file first?	no	+
	To turn on debugging, specify output file pathname	[ ]	
	DESCRIPTION of printer on remote server	[ ]	

F1=Help	F2=Refresh	F3=Cancel	F4=List
F5=Reset	F6=Command	F7=Edit	F8=Image
F9=Shell	F10=Exit	Enter=Do	

Now you are ready to print to Windows 2000 from AIX 5L. You can use almost all of the AIX 5L printing commands with this setup.

### 2.2.2 Using a remote printer attached to AIX 5L

In the second case, you are connected to a Window 2000 machine and you want to access a printer attached to an AIX 5L machine. The `lpr` and `lpd` commands are installed by default on AIX 5L, but not on Windows 2000 machines, so our first step is to install the necessary software. The `lpr` command is included in the Microsoft TCP/IP Print Server service. If this service is not installed on your system, refer to Section 2.2.1, “Using a remote printer attached to Windows 2000” on page 16 for installation information.

#### Note

TCP/IP Print Server service can be used for both client and server print service for UNIX. If you installed this service in Chapter 1, “Introduction” on page 1, you do not need to install it again.

Once this service is added to your machine, you need to add a new printer (if you have the proper authorizations to do so). Double-click on the **My Computer** -> **Control panel** icon, select the **Printers** panel, and double-click on the **Add Printer** icon, as shown in Figure 15 on page 20.



Figure 15. Control panel - Printers

The Add printer Wizard will be launched to assist you in this task, as shown in Figure 16. Select a local printer and uncheck the **Automatically detect and install my Plug and Play printer** check box.



Figure 16. Add Printer Wizard

The next panel requires that you select a port. Click on the **Create a New Port** button, select **LPR Port**, then click **Next**, as shown in Figure 17 on page 21.

If you followed the previous steps, one of the choices is LPR port (if it does not appear, it means you do not have Print Services for Unix).

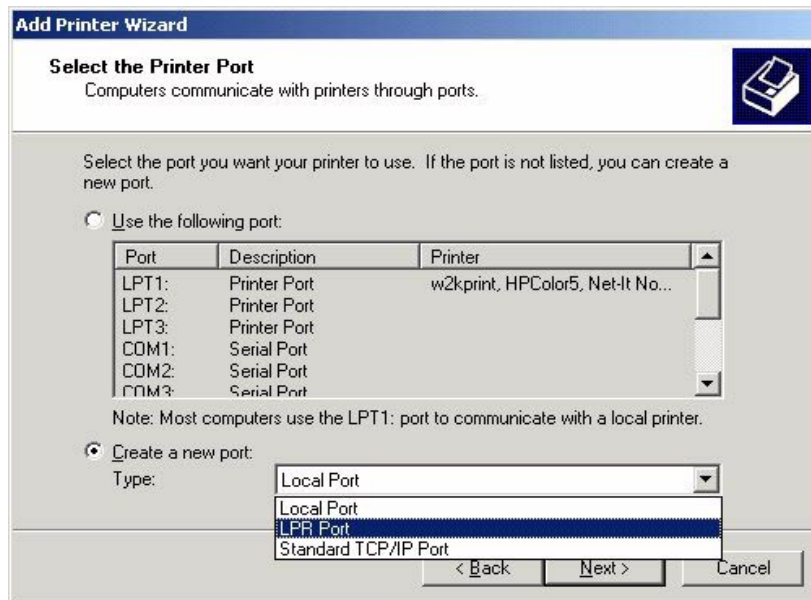


Figure 17. Select the LPR port

You are then prompted for the name or address of the server to which the printer is attached and the name of the remote queue, as shown in Figure 18 on page 22. The end of the configuration process is the same as adding a local or remote printer. You can now use this new print queue.

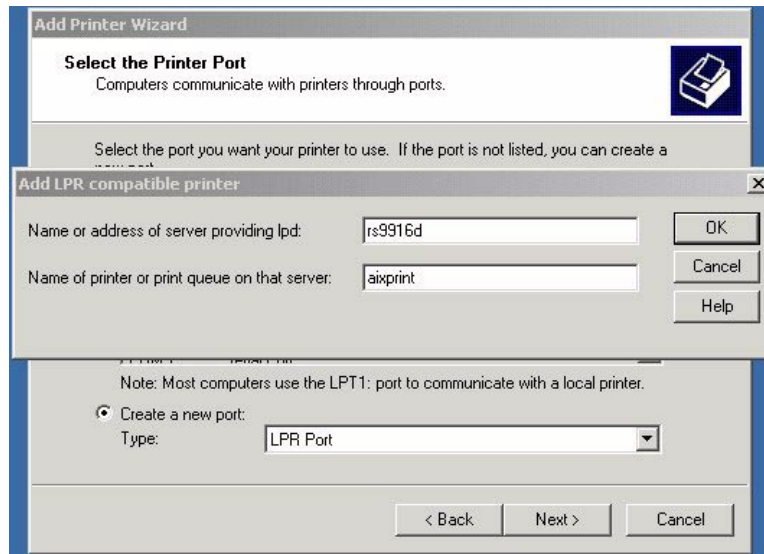


Figure 18. Add LPR compatible printer

Of course, on the AIX 5L machine, you must authorize the Windows 2000 machine to use the lpd daemon. In order to do that, you must add an entry to the `/etc/lpd/hosts` file for this machine or use the SMIT menu.

### 2.2.3 Using Web printing in Windows 2000

A new Web printing service has been added in Windows 2000. While it does not include interoperability between AIX 5L and Windows 2000, we feel that it is important for you to know about this feature, especially if you are maintaining printers in your company.

Web printing allows you to print out to a printer in your company from a remote machine, such as your home. The service uses the Web server installed on your Windows 2000 server or professional.

Once you have installed a printer in Windows 2000, use the following steps to use it from a remote machine:

**Note**

To access a printer via Web, you must have proper access permission. You will be prompted for a valid user ID and password.



Open your Web browser, and type one of the following in the address bar:

- If you do not know the printer's name, type using the format:

`http://PrintServerName/printers/`

Click on the name of a printer you want to connect to. For example, if the computer name of Windows 2000 is *w2kpro*, type `http://w2kpro/printers` to receive a page listing all the printers located on print server *w2ksrv*.

This will give you a list, as shown in Figure 19. Selecting one will take you to that printer's page, as seen in Figure 20 on page 24.

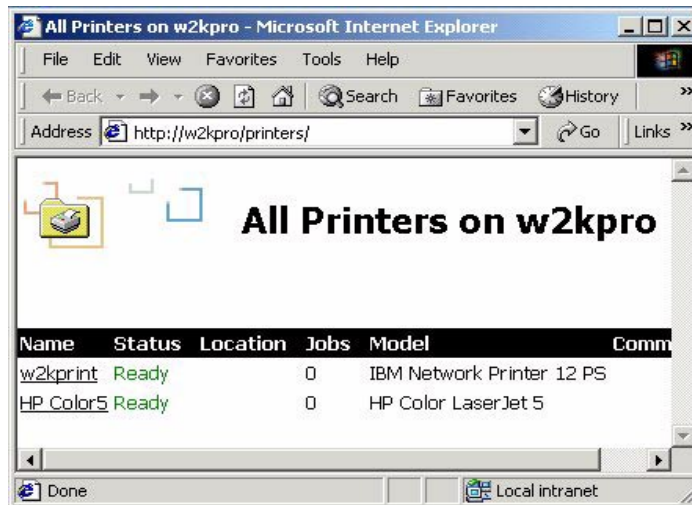


Figure 19. Locating printers via Web browser

- If you know the printer's name, type its URL using the format:

`http://PrintServerName/PrinterName/`

For example, type `http://w2kpro/HPColor5/` to go directly to that printer page (Figure 20 on page 24).

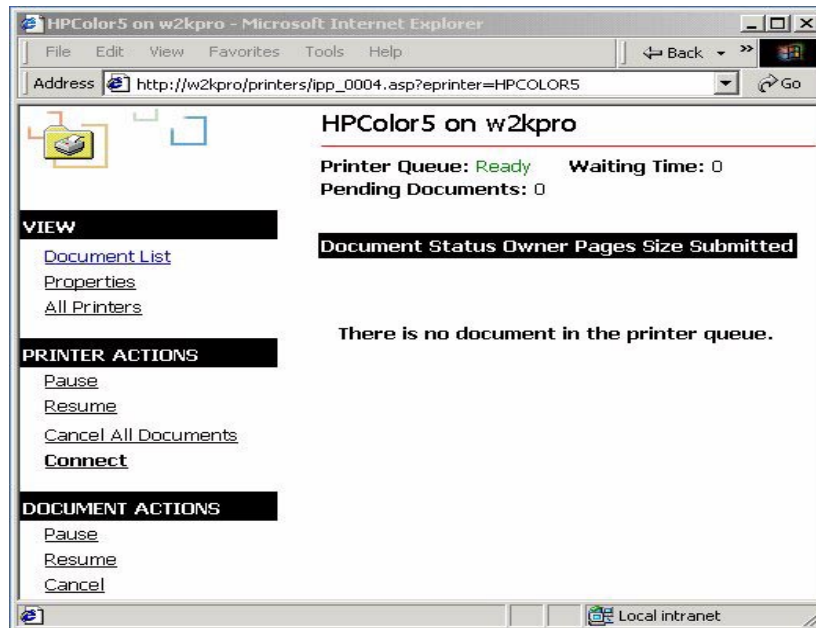


Figure 20. Printer management via Web browser

When viewing the printer's page, click **Connect** under **Printer Actions** to connect to that printer, as shown in Figure 20.

Windows 2000 automatically copies the appropriate printer driver to your computer, and the icon for the printer appears in your Printers folder, as shown in Figure 21 on page 25.

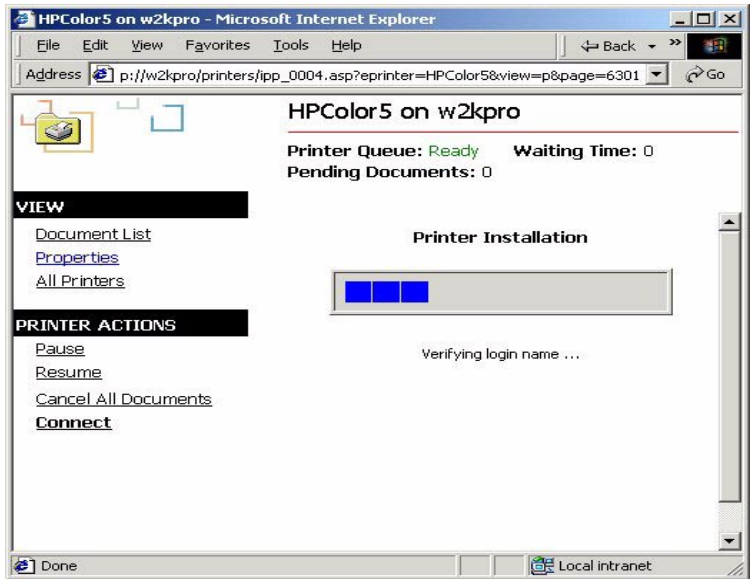


Figure 21. Printer driver installation in Web browser

If prompted, you will need to provide your valid user id and password, as shown in Figure 22.

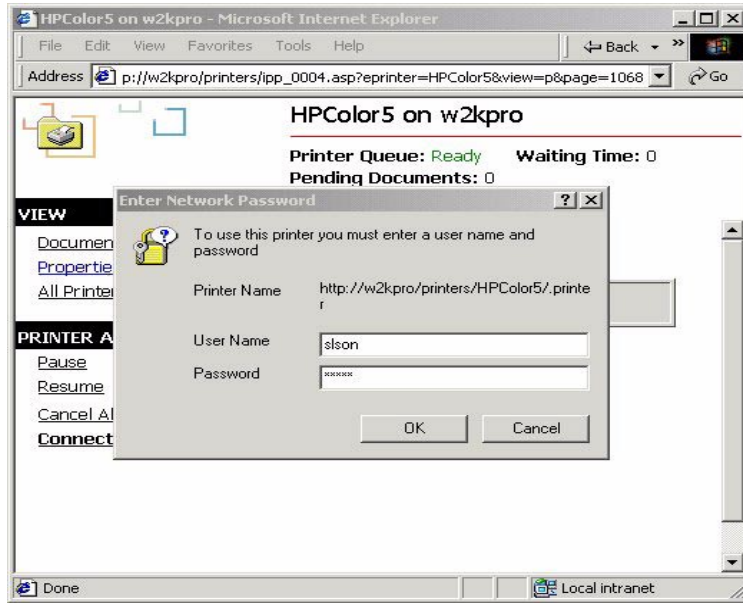


Figure 22. User authentication for installing a printer driver

If the installation is completed without any errors, Figure 23 is the final panel you will see.

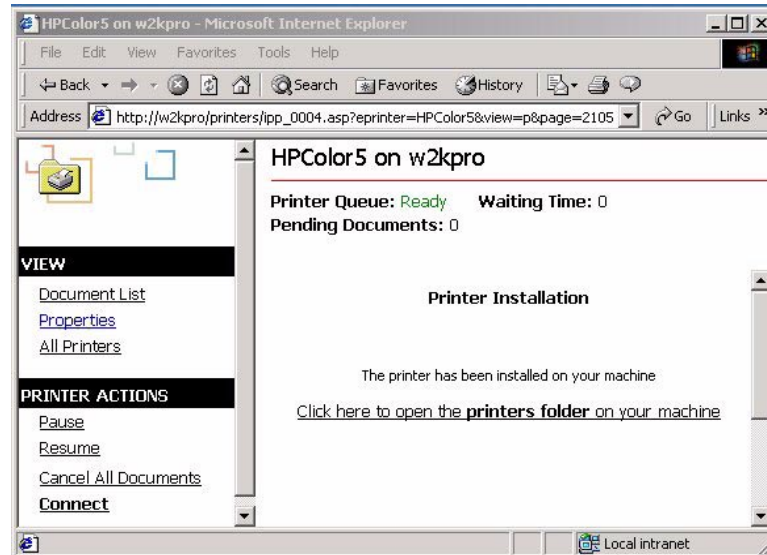


Figure 23. The final panel for installation of printer driver

---

## 2.3 Using Telnet

Telnet is a one of the most popular programs for interoperability between AIX 5L and the Windows family. For details, refer to Section 4.6, “Telnet components” on page 170.

### 2.3.1 Remote connection to AIX 5L machine

If you have a Windows 2000 machine, and want to access a remote AIX 5L machine, the process is very simple because the `telnet` command is included in the Windows 2000 operating system and the `telnetd` counterpart daemon is standard in AIX 5L. Just start the `telnet` command from your Windows 2000 machine (either from a DOS command-prompt or from any shortcut).

If you connect to AIX 5L from Windows 2000 client using `telnet`, you will see the following screen.

```

AIX Version 5
(C) Copyrights by IBM and by others 1982, 2000.
login: root
root's Password:
*****
*
*
* Welcome to AIX Version 5.0!
*
*
* Please see the README file in /usr/lpp/bos for information pertinent to
* this release of the AIX Operating System.
*
*
*****
Last login: Thu Feb  8 13:38:01 CST 2001 on /dev/dtlogin/_0

[YOU HAVE NEW MAIL]
#

```

Users of previous versions of Windows Telnet client may notice a few changes in the version included with Windows 2000. The most obvious change is that Telnet Client is now a command-line application rather than a Windows Application. As a command-line application, Telnet Client will seem very familiar to users of UNIX-based Telnet clients.

A major new feature found in Windows 2000 Telnet Client is NT LAN Manager (NTLM) authentication support. Using this feature, a Windows 2000 Telnet client can log on to a Windows 2000 Telnet server using NTLM authentication.

### 2.3.2 Remote connection to Windows 2000 machine.

The `telnet` connection to Windows 2000 from AIX 5L is not very useful because it is very difficult to manage the Windows 2000 system without a GUI. However, it can be used to interconnect. Refer to Section 4.6.1, “Telnet server” on page 171 for more information.

#### Note

Services for Unix is a product from Microsoft that you may find very useful if you are looking for an interoperability solution between AIX 5L and Windows 2000. Telnet server service is a part of the product.

---

## Chapter 3. PC connectivity solutions

This chapter introduces three products that provide interoperability between AIX 5L and the Windows 2000 family. All of these solutions use NetBIOS over TCP/IP, and the basic functions, including file and print sharing, are very similar to one another. We will explore the features and benefits of each solution so you can decide which one is appropriate for your network environment and business requirements.

---

### 3.1 AIX Fast Connect

In this section, we describe the overview of AIX Fast Connect Version 3.1 and connection setup between Windows 2000 and AIX 5L using AIX Fast Connect.

The complete documentation for AIX Fast Connect is located in the AIX 5L Version 5.1 Base Documentation.

#### 3.1.1 Overview

AIX Fast Connect is an IBM product that enables file and printer services on AIX systems for personal computer clients running Windows 2000, Windows NT, Windows 98, Windows 95, Windows for Workgroups, and OS/2 operating systems, as shown in Figure 24 on page 30. AIX Fast Connect server provides these services by implementing the Server Message Block (SMB) protocol on top of Network Basic Input/Output System (NetBIOS) over TCP/IP (RFC-1001/1002).

Because AIX Fast Connect uses industry standard Microsoft networking protocols, PC client can access AIX files and printers using their native networking client software.

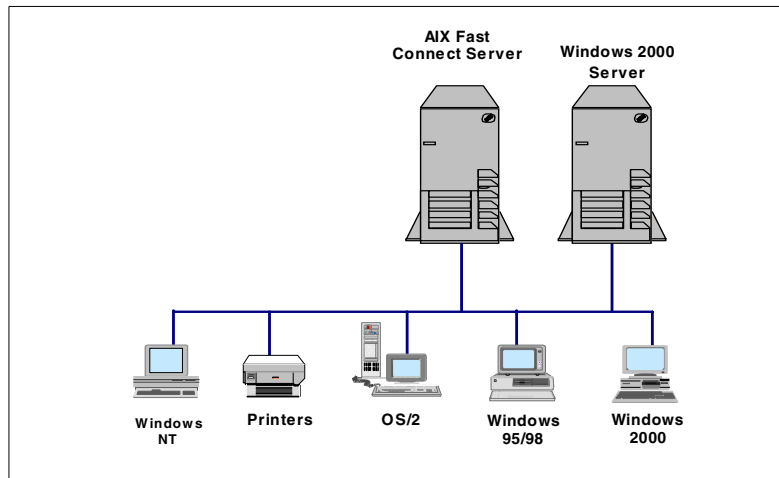


Figure 24. AIX Fast Connect server and supported clients

### 3.1.1.1 Features

AIX Fast Connect offers the following AIX application standard and advanced features:

- Tight integration with AIX using AIX features such as threads, kernel I/O, file system, and security
- Maintenance and administration using Web-based System Manager, SMIT, and command-line
- Streamlined configuration
- Trace and log capabilities
- SendFile API support
- DCE/DFS integration
- Support JFS-ACLs
- HACMP support using server name aliases

AIX Fast Connect provides Advanced SMB/NetBIOS features, including:

- SMB-based file and print services
- Passthrough authentication to Windows 2000
- Resource browsing protocol (Network Neighborhood or My Network Places)
- Network logon support, including roaming user-profiles



- WINS client and proxy, and NBNS server
- Opportunistic locking (oplock)
- B-node support
- Guest logon support
- Share level security support
- Message from server to client
- Mapping of AIX long filenames to DOS 8.3 filenames
- Unicode representation of share, user, file, and directory names
- Mapping of PC-client usernames to AIX usernames

### **3.1.1.2 Requirements**

The following sections describe the system requirements for configuring Windows clients and AIX servers using AIX Fast Connect.

#### ***Server hardware requirements***

AIX Fast Connect runs on any machine that supports Version 4.3.2 (or later) of the AIX operating system, except for diskless and dataless machines. This server machine must have the following hardware:

- 32 MB of RAM (a minimum of 64 MB is preferred)
- 50 MB of available disk space
- TCP/IP-supported LAN adapters physically connected to network

#### ***Server software requirements***

The following are the server software requirements for AIX Fast Connect:

- AIX Version 4.3.2 or higher.
- The size of /var file system should be large enough to temporarily store the largest file that can be printed by the print service.
- Fileset bos.net.tcp.client version 4.3.2.0 or higher must be installed and configured.
- Fileset bos.rte.loc version 4.3.2.2 or higher must be installed and configured.
- Fileset bos.up or bos.mp version 4.3.2.5 or higher is needed to support the SendFile API enhancement.

### ***Client hardware requirements***

Each client PC must have an installed LAN adapter, and should be physically connected to a network.

### ***Client software requirements***

To use AIX Fast Connect, all clients must have one of the following operating systems:

- Windows 2000 (with Service Pack 1 or higher)
- Windows NT 4.0 (with Service Pack 3 or higher)
- Windows 98
- Windows 95 (with Service Pack 1 or higher)
- Windows for Workgroups 3.11 or higher
- OS/2 Warp 4.0 or higher

To use the Web-based System Manager, a Web browser with forms support (for example, Netscape) is required.

### ***Known conflicts with other server software***

Like other NetBIOS servers, AIX Fast Connect cannot share ownership of the TCP/IP ports used for NetBIOS on a single machine. The NetBIOS-based server software listed in Table 1 is known to conflict with AIX Fast Connect. These products must be uninstalled before installing AIX Fast Connect. To identify if one of those products is installed, use the `ls1pp -l` command.

*Table 1. Other server software with known conflicts*

<b>Fileset</b>	<b>Description</b>
SAMBA	Samba Server
netbios.*	NetBIOS/ix for AIX
connect.*	AIX Connections
TAS.*	TotalNet Advanced Server for AIX
ASU.*	Advanced Server for UNIX

### 3.1.1.3 AIX Fast Connect packaging and installation

To install AIX Fast Connect, install the packages shown in Table 2.

Table 2. AIX Fast Connect packaging

Image	Description
cifs.base	Server utilities
cifs.client	Client utilities
cifs.msg.*	Server message (by language)
cifs.websm	Web-based System Manager Utilities
cifs.advanced-demo -or- cifs.advanced -or- cifs.basic	Demo Version (for Windows and OS/2 clients) Advanced Server (for Windows and OS/2 clients) Server (for Windows client only)

#### Note

The install files cifs.basic, cifs.advanced, and cifs.advanced-demo are mutually exclusive. Standard distribution of AIX Fast Connect contains only one of these images.

### Installation

To install AIX Fast Connect software on your AIX machine, you can use SMIT, the Web-based System Manager, or the `installp` command.

If you use SMIT, do the following:

1. Insert the AIX Fast Connect installation CD into your AIX machine.
2. On the command line, enter:  

```
# smitty installp
```
3. Select **Install Software**.
4. Define the input device as the CD-ROM device.
5. You will see following screen. Choose the filesets needed for your environment using the F4 key. To continue the installation, press the Enter key.

Install Software

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

[Entry Fields]

```

* INPUT device / directory for software      /dev/cd0
* SOFTWARE to install                       [cifs.base      > +
PREVIEW only? (install operation will NOT occur)  no          +
COMMIT software updates?                     yes         +
SAVE replaced files?                         no          +
AUTOMATICALLY install requisite software?     yes         +
EXTEND file systems if space needed?         yes         +
OVERWRITE same or newer versions?           no          +
VERIFY install and check file sizes?        no          +
Include corresponding LANGUAGE filesets?     yes         +
DETAILED output?                            no          +
Process multiple volumes?                   yes         +
ACCEPT new license agreements?              no          +
Preview new LICENSE agreements?             no          +

```

F1=Help      F2=Refresh      F3=Cancel      F4=List  
F5=Reset      F6=Command      F7=Edit      F8=Image  
F9=Shell      F10=Exit      Enter=Do

Installation of AIX Fast Connect creates the files shown in Table 3 on the server.

Table 3. AIX Fast Connect files

File	Type	Path	Description
net	binary	/usr/sbin	Command-line administration command
cifsClient	binary	/usr/sbin	Command-line utility for sending messages to PC clients
rc.cifs	script	/etc	Start/stop shell script
cifsServer	binary/link	/usr/sbin	Main server daemon (one main server process, owned by root)
cifsServerAdv	binary	/usr/sbin	Main server daemon (from cifs.advanced)
cifsServerAdvDemo	binary	/usr/sbin	Main server daemon (from cifs.advanced-demo)
cifsUserProc	link	/usr/sbin	Client-session daemon (one process per PC-client session)
cifsPrintServer	binary	/usr/sbin	Print server daemon

File	Type	Path	Description
cifsPrintServerDCE	binary	/usr/sbin	Print server daemon (for DCE/DFS support)
cifsConfig	text	/etc/cifs	Server configuration file
cifsPasswd	text	/etc/cifs	User-database file
README	HTML	/etc/cifs	Additional documentation
cifsLog	text	/var/cifs	Log file
cifsTrace	text	/var/cifs	Trace file
sm_smb.cat	message catalog	/usr/lib/nls /msg	Runtime message catalogs (by language)

**Note**

- For DCE/DFS support, you must install `dce.client.*` before installing AIX Fast Connect.
- The `cifsTrace` file does not appear on the system until tracing is enabled using the `net trace` command.

### **Configuration of network interface**

Whenever the AIX Fast Connect server is started, it automatically supports RFC1001/1002 (NetBIOS over TCP/IP) on all AIX TCP/IP interfaces that are currently defined and operational. No special or additional configuration is required to support these interfaces.

### **Initial configuration**

During installation, AIX Fast Connect preconfigures itself as an SMB/NetBIOS file server with the default parameters shown in Table 4.

*Table 4. AIX Fast Connect default parameter values*

Parameter	Initial value
servername	hostname (TCP/IP hostname)
comment	"Fast Connect server on hostname"
domainname	WORKGROUP
encrypt_passwords	0 (Plain text passwords)

Parameter	Initial value
guestlogonsupport	0 (disabled)
networklogon	0 (disabled)
share_level_security	0 (disabled)

In addition, the HOME file share is predefined. It maps to \$HOME, the AIX Connect user's home directory on AIX.

Other server parameters are initially at the default values.

### 3.1.2 AIX Fast Connect configuration and administration

This section describes basic configuration and operation of AIX Fast Connect. You can use the Web-based System Manager, SMIT, or the `net` command to configure and administer the AIX Fast Connect server for your site. Any user can access the AIX Fast Connect Server configuration menu, but only the root user is allowed to change it. As mentioned in Section 3.1.1, "Overview" on page 29, AIX Fast Connect preconfigures itself to provide basic access to AIX users' home directory (as defined in `/etc/passwd`) using plain-text network passwords.

#### 3.1.2.1 Example configuration and system environment

To illustrate the configuration process, we use the example configuration and system environments shown in Figure 25 on page 37.

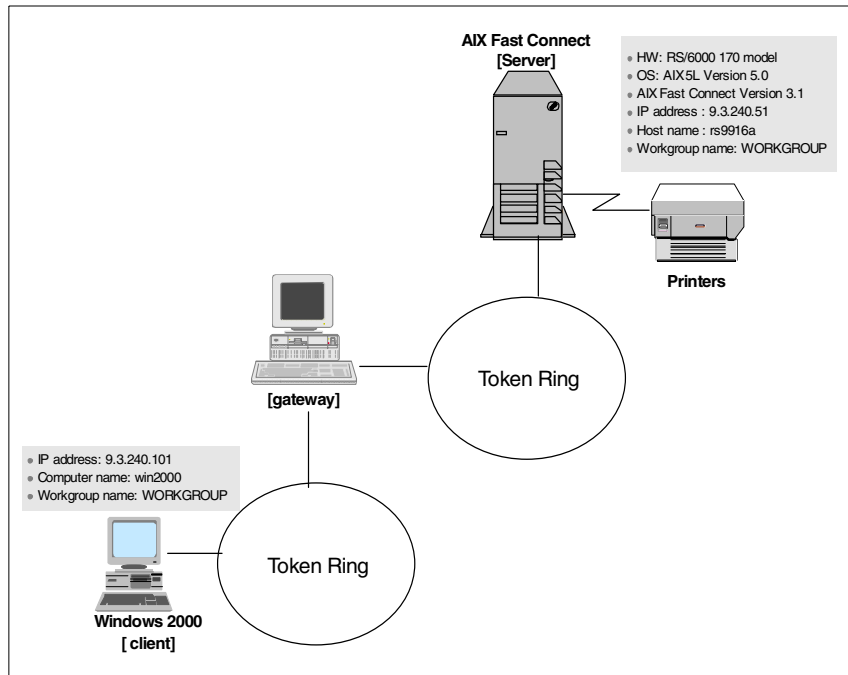


Figure 25. Example of AIX Fast Connect configuration and system environments

### 3.1.2.2 Starting and stopping the Fast Connect Server

When the AIX Fast Connect product is installed on the system, you can start the server without any additional configuration.

You have three options for starting the server:

#### **Option 1: From Web-based System Manager**

1. Click **PC Services (Fast Connect)**.
2. Click **Overview and Tasks**.
3. Click **Start local Fast Connect server operations**.
4. The pop-up panel shown in Figure 26 on page 38 will open.
5. Click the **OK** button to complete these steps.

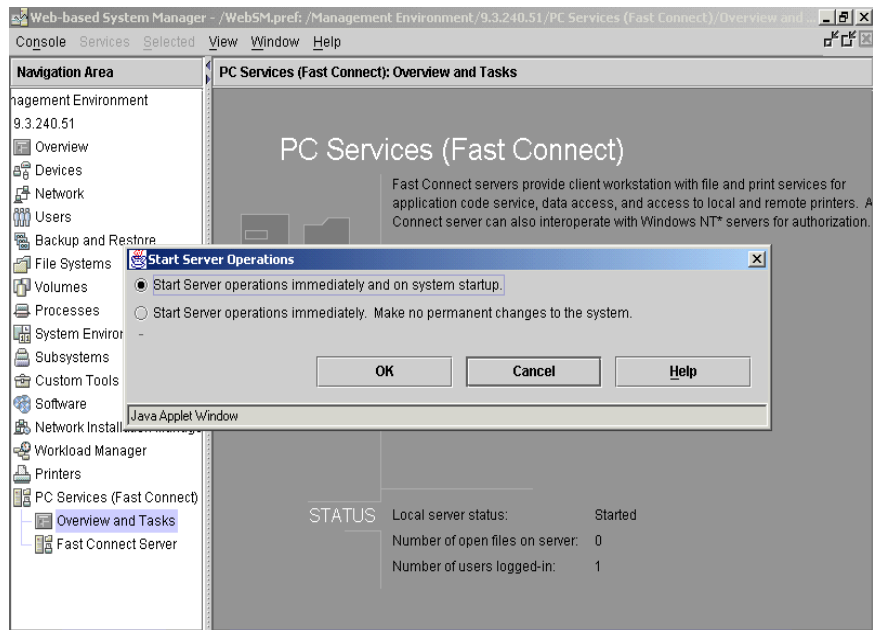


Figure 26. Starting AIX Fast Connect server using Web-based System Manager

**Option 2: From SMIT**

1. Enter the following command from the command line:

```
# smitty smb
```

2. Select the **Start Server** option.

**Option 3: From the command line**

Enter the following command:

```
# net start /load
```

To stop the server, you also have three options:

**Option 1: From Web-based System Manager**

1. Click **PC Services (Fast Connect)**.
2. Click **Overview and Tasks**.
3. Click **Stop local Fast Connect server operations**.

**Option 2: From SMIT**

1. Enter the following command from the command line:

```
# smitty smb
```



## 2. Select **Stop Server**

### **Option 3: From the command line**

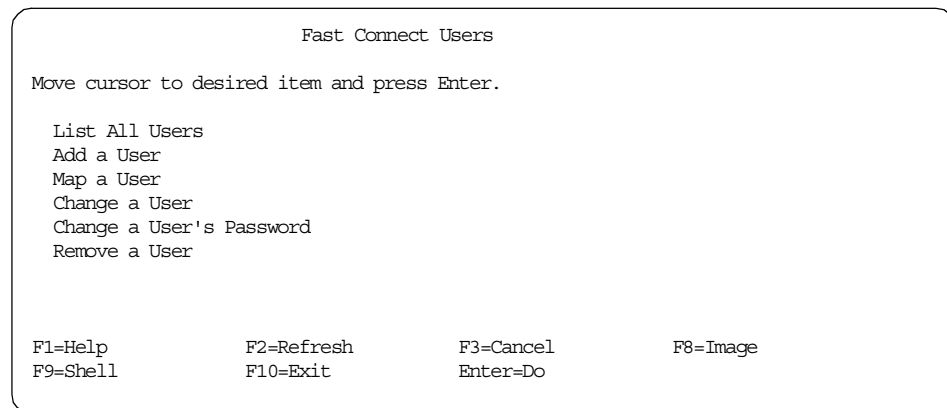
Type the following command:

```
# net stop
```

From Web-based System Manager, you can see that the server is running when the Status label is Started. From the command line, you can use the `net status` command to check the status of the server.

### **3.1.2.3 User Administration**

When a client requests a connection to the server, the client's username and password are compared to the server user's name. You can add new users, and modify and delete existing users. You can also activate and deactivate a user. The following screen shows the SMIT menu (SMIT fast path `smbcfgusr`) to administer Fast Connect user.



At the command line, type the following command:

```
# net user [ /add | /delete ]
```

#### **Note**

All AIX Connect users must also be AIX users. You cannot add a new Fast Connect user if this user does not exist as an AIX user.

### **3.1.2.4 Configuration of File and Print Shares**

There are two types of shares that can be configured and exported with AIX Fast Connect: File shares and Print shares.

Whenever the AIX Fast Connect server is started, a file share with the network name HOME is created by default. This special file share maps to \$HOME, the AIX home directory (from /etc/passwd), of any PC-client user that connects to AIX Fast Connect.

**Note**

The default share HOME cannot be changed or deleted.

Each file or print share represents an object that AIX Fast Connect is exporting to the Windows network. Each is accessed by its netname. File shares are exported AIX directories. Print shares are exported AIX print queues.

- To list all shares currently exported by AIX Fast Connect, type the following command:

```
# net share
```

- To add a new file share (for example, to export AIX directory /tmp as network-name NETTEMP), type the following command:

```
# net share /add /type:f /netname:NETTEMP /path:/tmp /desc:"File share"
```

- To add a new printer share (for example, to export AIX print queue prt1 as network name PSPRT1), type the following command:

```
# net share /add /type:p /netname:PSPRT1 /printq:prt1 /desc:"Print share"
```

**Note**

AIX name for files, directories, and print-queues are case-sensitive, but network-names used by Windows networking are not.

- To delete a share (for example, the share NETTEMP listed above), type the following command:

```
# net share /delete /netname:NETTEMP
```

### 3.1.2.5 Basic server administration

The following sections show basic server operations using the AIX Fast Connect `net` command:

- To load the server-daemon, and enable PC-clients to connect, type the following command:

```
# /etc/rc.cifs start
```

- To stop the server and unload the server-daemon, type the following command:

```
# /etc/rc.cifs stop
```

**Note**

When the server-daemon (cifsServer) is not loaded, the AIX Fast Connect `net` command does not function. To configure AIX Fast Connect parameters offline, you might need to load the server daemon manually by typing `/user/sbin/cifsServer` on the command line. This enables the `net` command, but does not start the server. PC clients are not able to connect until the `/etc/rc.cifs start` command is issued.

- To temporarily reject new SMB-sessions (without disturbing the existing connection), type the following command:

```
# net pause
```

- To re-enable the server to accept new connections, type the following command:

```
# net resume
```

- To query the server's operational status, type the following command:

```
# net status
```

- To show general configuration information, type the following command:

```
# net config
```

- To show statistical information, type the following command:

```
# net statistics
```

- To query the status of logged-in user-session, type the following command:

```
# net session
```

### 3.1.3 Accessing AIX Fast Connect Server from Windows 2000

As we mentioned in Section 3.1.1, "Overview" on page 29, we can use Windows 2000, Windows NT, Windows 98, Windows 95, Windows for Workgroups, and OS/2 operating systems as clients of the AIX Fast Connect Server. In this section, we discuss the steps required to connect Windows 2000 clients to AIX Fast Connect Server.

### 3.1.3.1 Configuring Windows 2000

Before you start to configure Windows 2000, make sure that you have installed the Workstation service and the TCP/IP protocol. Also, check that you are logged on as administrator or as a user who is included in the local administrators group.

#### **TCP/IP Configuration**

1. From the **Start** button, select **Settings -> Control Panel -> Network and Dial-up Connections**.
2. Right-click on the **Local Area Connection** icon of the network adapter to be configured. Select **Properties**.
3. In the General tab, shown in Figure 27, verify that there are checked entries for the following components:
  - Your networking card (hardware driver) entry
  - Client for Microsoft Networks
  - Internet Protocol (TCP/IP)

If any are missing, add them from your Windows 2000 CD.

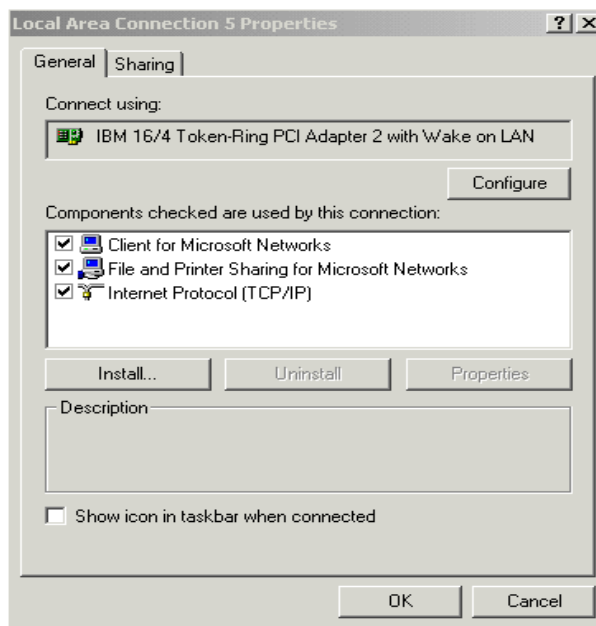


Figure 27. Windows 2000 Local Area Connection Properties

4. Select the **TCP/IP** entry, then select the **Properties** button. Configure as needed. (For initial testing, you may want to disable DHCP and manually specify unique IP address for each PC.)
5. Select **Advanced**.-> **WINS**, to verify that NetBIOS over TCP/IP is enabled.
6. Test the client's TCP/IP configuration using the `ping` command, using the IP address from the client PC's DOS prompt to the AIX Fast Connect server, and vice versa.

### **Identification changes**

1. From the **Start** button, select **Settings** -> **Control Panel**, and then double-click the **System** icon.
2. On the System Properties dialog box, select the **Network Identification** tab and click the **Properties** button. You should see the dialog box shown in Figure 28.

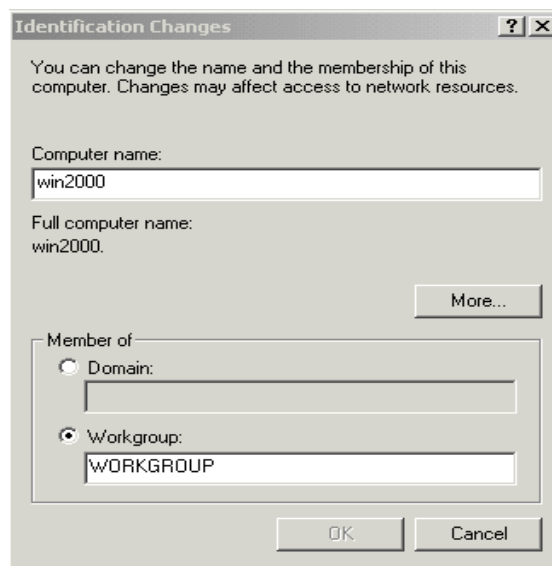


Figure 28. Identification changes

3. Enter your computer name. Next, click the Workgroup radio button and enter the workgroup name, which should match the one you set up in your AIX Fast Connect server.
4. You will need to reboot in order for the changes to take effect.

### 3.1.3.2 Locating the AIX 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

#### **Option 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.
6. You will see the Fast Connect server that you configured (Figure 29).

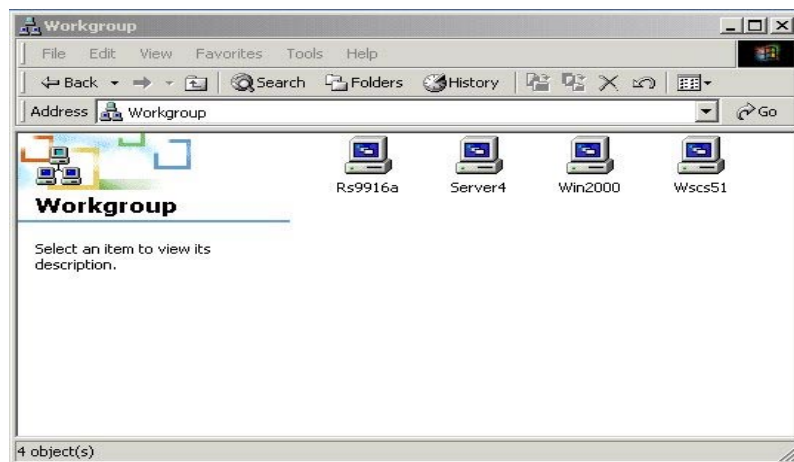


Figure 29. Browsing Workgroup

#### **Option 2: Locating the server with the Search for Computer option**

You can use the Find computer option to locate 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 Computers** link on the left.
4. Enter the computer name (the server name of AIX Fast Connect Server).
5. Click the **Search Now** button.
6. You will see the Fast Connect server (Figure 30).

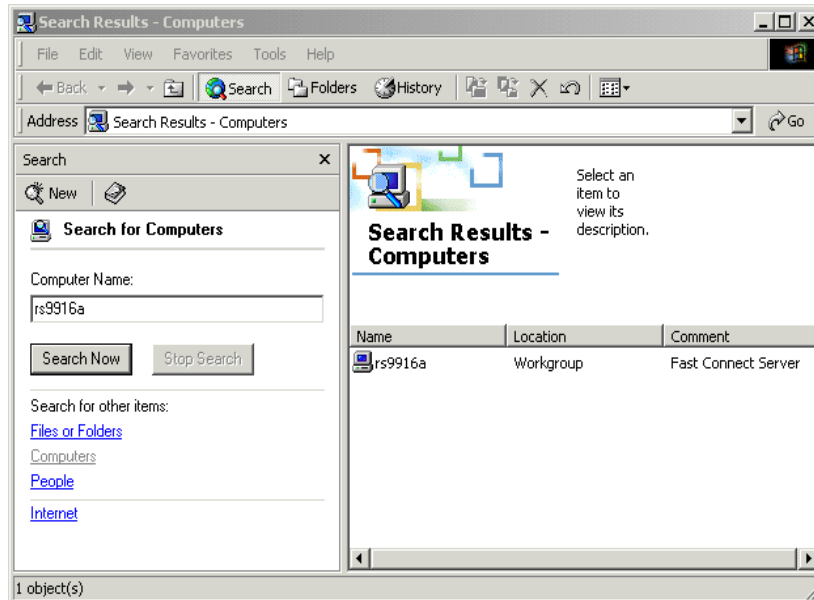


Figure 30. Search Results - Computers

### **Option 3: Locating the server from the command line**

You can use the `net view` command to locate the server. 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>` (server name is the name of the Fast Connect Server whose resources you want to share), or type `net view /DOMAIN:<domainname>` (domain name is the name of the domain where your Fast Connect server is included).

The following screens show the execution of these two commands.

```

C:>net view \\rs9916a
Shared resources at \\rs9916a

Fast Connect Server

Share name      Type          Used as      Comment
-----
HOME            Disk          User's Home  Directory Share
SH_SOFTWARE     Disk          Share software
The command complete successfully

```

```

C:>net view /DOMAIN:workgroup
Server Name      Remark
-----
\\RS9916A        Fast Connect Server
\\SERVER4        Fast Connect Server
\\WIN2000
\\WCS51
The command complete successfully

```

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

### 3.1.3.3 Accessing resources from the AIX Fast Connect Server

This section describes how to connect a Windows 2000 client to an AIX Fast Connect server.

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

#### ***Option 1: Using the GUI interface***

When you want to access the network shared resources 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 **My Network Places** 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 **Entire Contents** text.
4. Click the **Microsoft Windows Network** icon.



5. Click the domain of your Fast Connect server.
6. Double-click the server name of your Fast Connect server (rs9916a in this example).
7. You will see the shared resources of the rs9916a server as shown in Figure 31.

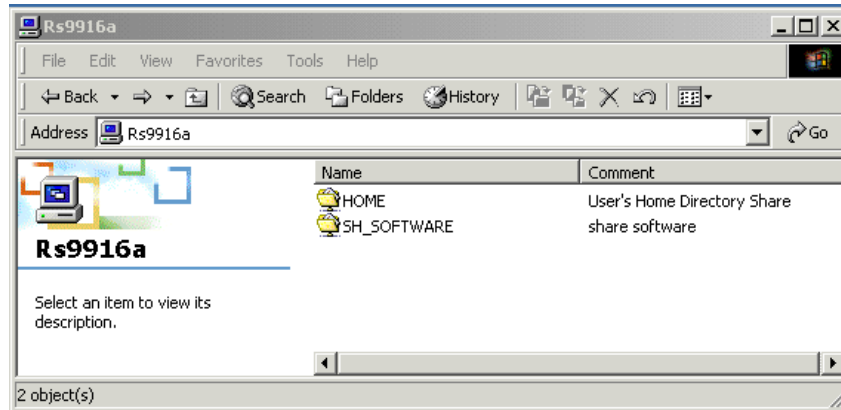


Figure 31. AIX Fast Connect shared resources

8. Click the shared resource (for example, sh\_software) and select **File -> Map Network Drive...**, or right-click the shared resource and select **Map Network Drive...**
9. Select the desired drive (for example, X:)
10. Click the **Finish** button (see Figure 32 on page 48).

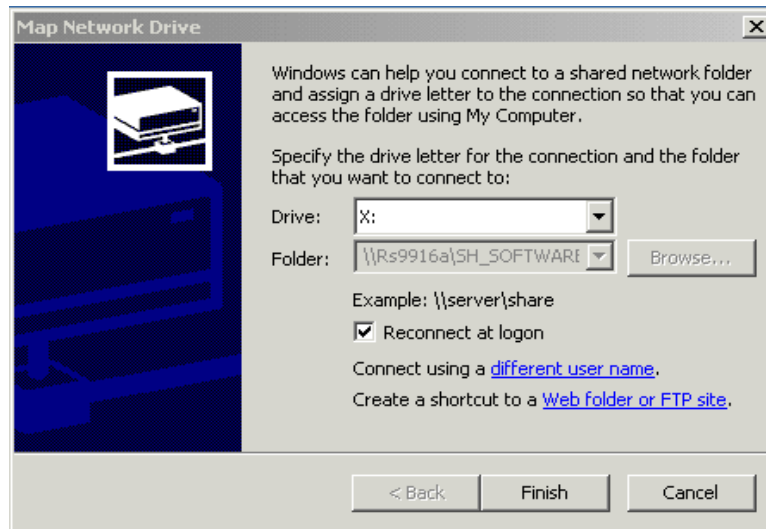


Figure 32. Map Network Drive

### **Option 2: Using the command line interface**

We can also map a network drive to the shared resources from the DOS command prompt using the `net use` command.

You can use the `net use` command without parameters to see the current status of mapped shares, as shown in the next screen.

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

Status      Local      Remote          Network
-----
The command completed successfully.
```

In the next screen, you can see the creation of a network drive, X:, which is connected to share SH\_SOFTWARE on the rs9916a computer.

```
C:\>net use x: \\rs9916a\SH_SOFTWARE /user:ausres21
The command completed successfully.
```

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

Status	Local	Remote	Network
OK	X:	\\rs9916a\SH_SOFTWARE	Microsoft Windows Network

```
The command completed successfully.
```

You can delete the network mapping with the /delete option:

```
c:> net use x: /delete
```

### 3.1.4 AIX Fast Connect problem determination

This section describes Fast Connect specific tools and activities for locating the problem with the SMB/CIFS protocol.

#### 3.1.4.1 Connection checking procedure

1. Use the `ping` command to the AIX Fast Connect server by IP address. If a timeout occurs, check:
  - The cable for physical connection
  - The status of the AIX machine
  - The TCP/IP configuration on clients and on the AIX server
2. Use `ping` on the AIX Fast Connect server with its NetBIOS name.
3. Check server status on the AIX machine using `net config`, `net status`, and `net statistics`.

#### 3.1.4.2 Net statistics

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

```

Server rs9916a is running on rs9916a
Since Tue Feb  6 10:51:28 CST 2001

Server statistics since Tue Feb  6 10:51:28 CST 2001

Sessions started                2
Sessions timed out             0
Sessions dropped                2
Password Errors                 0
Permission Errors              0
Bytes sent low                  5258
Bytes sent high                 0
Bytes received low              6518
Bytes received high             0
Request buffer failures         0
Big buffer failures            0
Print jobs queued              0

```

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

- Session 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.
- 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. Even if this number is not zero, it does not necessarily imply a security alert, as the number may indicate the quest account was used or somebody mistyped a password. The first step is for the client to send the user's name and password, which can be rejected (therefore 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 monitor net statistics output if you enter the following:

```
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 outputs. 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; later, you can see more dropped (ended) sessions than started ones.

### 3.1.4.3 Trace

The AIX trace facility helps you isolate system problems by monitoring selected system events. When a trace facility is active, information about selected events is recorded in the trace file. AIX Fast Connect server supports trace facility with the events (trace hooks) shown in Table 5.

Table 5. AIX Fast Connect trace hooks

Trace hook ID	Description
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

Trace files can be created by using either through SMIT or the `trace` command.

An example of the use and output of `trace` command is shown in the following output.

```

# trace -a -j 2EE,2EF,2F0,2F1,2F2,2F3,2F4,2F5 -o /tmp/trace.out
# sleep 30; trcstop
# trcrpt -t /etc/trcfmt /tmp/trace.out

Tue Feb  6 14:18:15 2001
System: AIX rs9916a Node: 5
Machine: 000FA16D4C00
Internet Address: 0903F033 9.3.240.51
The system contains 1 cpus, of which 1 were traced.
Buffering: Kernel Heap
This is from a 32-bit kernel.

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

ID      ELAPSED_SEC      DELTA_MSEC      APPL      SYSCALL  KERNEL  INTERRUPT
001      0.000000000      0.000000      TRACE ON channel 0
          Tue Feb  6 14:18:15 2001
2EE      4.798624128      4798.624128      CIFS Enter LS_NBProcNSDGram
2F2      4.798669456      0.045328      CIFS-NET data 32804 string 9.3.240.101
2F2      4.798699530      0.030074      CIFS-NET data 32818 string ITSONT02
2EF      4.889955467      91.255937      CIFS Exit NBaccept socket=4

```

As you can see from the previous screen, the trace output shows detailed information and the internal flow of AIX Fast Connect Server, such as its IP address and the elapsed time for all steps.

#### 3.1.4.4 Logs

The AIX Fast Connect server writes informational and error messages to a file in /var/cifs named cifsLog, as shown in the next screen. You can see the detail error numbers when the Fast Connect Server has any problem. In this case, there is a problem related to Passthrough servers's IP address.

```

Thu Mar  1 11:26:38 2001

Probe Event:      handlePassAuthNegP
Probe Function:   810
Probe Location:   9
Warning: PassThruServer's IPAddress is invalid,

```

### 3.1.5 Migrating to AIX Fast Connect from AIX Connections

For AIX Connections users to migrate to AIX Fast Connect, netbios.\* filesets must be uninstalled, which also requires the connect.\* prerequisite filesets to be uninstalled.

Before uninstalling AIX Connections (ACONN), you might want to save the old configuration files. These are plain text configuration files that can be used as a reference when configuring AIX Fast Connect.

Table 6 lists the AIX Connections (connect.\*) configuration files.

Table 6. AIX Connection configuration files

Configuration file	Description
/usr/tn/config.tn	Network/socket definitions
/usr/tn/profile.file	Export/share definitions
/usr/tn/services.NB	Service definitions for NB-realm
/usr/tn/services.NW	Service definitions for NW-realm
/usr/tn/services.AT	Service definitions for AT-realm
/usr/tn/.lic.toc	Number of licensed users
/usr/tn/passwd.file.narrow	Encrypted passwords

To save these configuration files before uninstalling ACONN, simply copy/move these files to new names, for example, config.tn.save.

In Table 7, you can see the NetBIOS/ix (netbios.\*) configuration files.

Table 7. NetBIOS/ix configuration files

File name	Description
/etc/msctab	LANA definitions
/etc/mcs0	startup script (possibly customized)
/etc/mscnet/wins.names	WINS data
/etc/inethosts	NIP cache (similar to LMHOSTS)

To save NetBIOS configuration data, the saved filename must not begin with mcs, because netbios.\* deletes all mcs\* filenames during its uninstall process.

### 3.1.6 Performance considerations

This section discusses several issues affecting AIX Fast Connect performance.

#### 3.1.6.1 Large directories

Directory enumerations are frequent network operations on Windows clients. Whenever Network Neighborhood or My Network Places (or Windows Explorer) opens a network directory, the entire directory is enumerated over the network for display in a Explorer panel. For large directories containing many files, this delay is noticeable to the PC user, and can be frustrating. Remote file accesses from AIX (such as DCE/DFS or NFS) tend to aggravate this situation.

To keep your AIX Fast Connect users from having to access large directories to get to the network files they need, you may define smaller-sized AIX directories to be exported by AIX Fast Connect. These directories can contain links to files in the large directories.

#### 3.1.6.2 Search caching

Directory searches are very frequent network operations on Windows clients. Every time a network file is opened, renamed, deleted, or listed, a directory search for that filename is performed. For example, simply opening a document in Microsoft Word can cause multiple directory searches for that filename.

AIX Fast Connect has a search-caching feature that allows directory searches to be temporarily cached to improve the performance of multiple-search scenarios, such as opening documents. Also, for directories that change infrequently, but are accessed often, this feature enhances performance.

Search caching is implemented in AIX Fast Connect by taking snapshots of directories and their modification times.

Search caching is configured on AIX Fast Connect by several parameters, as shown in Table 8.

Table 8. Search cache parameters

Parameter	Default	Description
cache_searches	0 (disabled)	Globally disables the search-caching feature.
sh_searchecache	0 (disabled)	Disables search caching on a per-share basis.



### 3.1.6.3 SendFile API support

For file transfers to clients, AIX Fast Connect can use the SendFile API for performance enhancement. The SendFile API is an AIX kernel extension that provides efficient file transfers and can do data caching.

SendFile API is configured on AIX Fast Connect by several parameters. To enable SendFile API on any file shares, the *send\_file\_api* must be enabled, and *sh\_sendfile* must be enabled for every file share for which SendFile API support is desired.

### 3.1.7 Limitations

The following limitations apply to AIX Fast Connect:

- The maximum file size is 4 GB (individual files must be less than 4 GB).
- All AIX usernames that access AIX Fast Connect must have an AIX home directory specified. Otherwise, access is not granted.
- Users of OS/2 or other clients that do not support Unicode must ensure that client and server locales match.
- Disk quota and ulimit are not checked for each user. A single user can fill the shared file system.
- AIX Fast Connect does not allow multiple printer share names for a single AIX print queue name.
- Some AIX back-end printer drivers add controls to the file being printed, while others do not. Windows clients always send print jobs in a format that needs no controls. So, if your AIX printer driver adds controls, you must set the *-o -dp* printer share options when you create the printer share.
- Guest Logon support is mutually exclusive to DCE/DFS authentication. Also, Guest Logon support is mutually-exclusive to NT Domains Passthrough Authentication.
- Network Logon support is mutually exclusive to NT Domains Passthrough Authentication.
- Network Logon is supported for Windows NT clients only through IBM Network Primary Logon Client for Windows NT (see [http://service.boulder.ibm.com/asd-bin/doc/en\\_us/winntcl2/f-feat.htm](http://service.boulder.ibm.com/asd-bin/doc/en_us/winntcl2/f-feat.htm)). Network Logon is not supported for Windows 2000.
- Share names and comments can only be in ASCII.

The *LC\_MESSAGES=C@lft* environment variable does not support multi-byte characters. If AIX Fast Connect is running in a multi-byte

environment and LC\_MESSAGES is set to C@lft, either unset it or set this variable to the correct locale at the beginning of the AIX Fast Connect program.

---

## 3.2 Samba

Samba is freeware that was originally developed by Andrew Tridgell at the Australian National University in 1990. Since that time, many other contributors have worked on this project.

Samba is very popular freeware that turns your AIX 5L machine into a resources server for your PC clients. In this section, we will describe how to install and set up a Samba server (Version 2.0.7), and how to declare file and printer shares.

### 3.2.1 Overview

Samba is a open source software suite that provides file and print services to Server Message Block (SMB) /Common Internet File System (CIFS) clients. Samba implements the SMB/CIFS protocols that enable clients and servers to exchange messages and data. Samba enables UNIX systems to act as file and print servers for PC client systems. Although Samba is primarily used to provide Windows-like files and print services under UNIX, it also includes UNIX SMB client utilities.

Windows 2000 family (including Windows ME and Windows 9x) do not need any extra software to access a Samba server. These operating systems all support NetBIOS over TCP/IP, which is all that is needed to access a Samba server.

#### Note

CIFS is an enhanced version of Microsoft's open, cross-platform SMB protocol, the native file-sharing protocol in the Windows 95, Windows NT, and OS/2 operating systems, and the standard way that millions of PC users share files across corporate intranets. CIFS is also widely available on UNIX, VMS, and other platforms.

Microsoft is making sure that CIFS technology is open, published, and widely available for all computer users. Microsoft submitted the CIFS 1.0 protocol specification to the Internet Engineering Task Force (IETF) as an Internet-Draft document.

### 3.2.2 NetBIOS and SMB overview

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

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

NetBIOS operated over proprietary Sytec protocols on IBM's PC Network, an early form of broadband LAN technology that accommodated up to 72 connected devices. From its early origins, it is important to emphasize that NetBIOS was not designed to scale and grow into use in large networks.

Prior to Windows 2000, all MS-DOS and Windows-based operating systems required the NetBIOS naming interface to support network capabilities. With the release of Windows 2000, support for the NetBIOS naming interface is no longer required for networking computers.

For example, an environment consisting of host computers and programs that support the use of the Domain Name System (DNS) could be built to run using Windows 2000 and other operating systems not requiring NetBIOS names, such as some versions of UNIX. However, most networks still need to integrate legacy operating systems that require NetBIOS network names with computers running Windows 2000.

For this reason, Windows 2000 provides default support for NetBIOS names. This support is provided mainly in two ways:

- By default, all Windows 2000 computers that use TCP/IP are enabled by default to provide client-side support for registering and resolving NetBIOS.
- Windows 2000 Server continues to provide server-side support through Windows Internet Name Service (WINS). WINS can be used to effectively manage NetBT-based networks.

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

NetBIOS over TCP/IP uses the three TCP/IP ports listed in Table 9.

Table 9. TCP/IP ports used by NetBIOS over TCP/IP

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

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

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

**Note**

In many cases, it is very difficult for you to understand the concept of NetBIOS name and SMB protocol. Simply speaking, NetBIOS name often means Computer name in Windows 2000, and SMB is a protocol that is used for file and print sharing.

### 3.2.3 Obtaining Samba

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

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

Samba is available at the following sites:

<http://www.samba.org>

<http://www.samba.org/samba/ftp/samba-latest.tar.gz> (the most recent version)

<http://www-frec.bull.com/docs/download.htm> (in AIX installp format)

<ftp://ftp.samba.org/pub/samba>

<ftp://ftp.samba.org/pub/samba/samba-latest.tar.gz> (latest version)

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

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

<http://www.cvshome.org>

**Note**

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

### 3.2.4 Samba support

Using the Internet is the most popular way to get support for Samba. Various Web sites provide information to assist administrators in solving Samba problems themselves. Documentation for Samba can be found at:

<http://www.samba.org/samba/docs/>

Increasingly, however, commercial support is available for those who require it. The following Samba Web site lists over 150 companies around the world that offer support for Samba on a commercial basis:

<http://www.samba.org/samba/support/>

### 3.2.5 Quick installation

In this section, we discuss how to quickly install the Samba server using the installp binary for Samba. You will need to download the Samba installp freeware code and install the code. You can take following steps in an AIX 5L machine:

1. Download Samba from the Web site.
2. Enter # `chmod 755 SAMBA-2.0.7.0.exe`.
3. Enter # `./SAMBA-2.0.7.0.exe`.
4. Enter # `inutoc`.
5. Enter # `smitty install`.

The installation process modified `/etc/services` and `/etc/inetd.conf`.  
`/etc/inetd.conf` now includes the `smbd` and `nmbd` entries.

After the installation, the following directory structure exists:

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

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

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

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

To use SWAT, the Web-based Samba administration interface, follow these steps:

1. Uncomment SWAT in the `/etc/inetd.conf` file.
2. Enter # `refresh -s inetd`.

Please note that SWAT (Samba Web Administration Tool) will modify the Samba configuration file, which is stored in `/usr/local/lib/smb.conf`.

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

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

and log in as root using the ordinary AIX password.

### 3.2.6 Configuring the Samba daemons

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

The `smbd` process provides LAN Manager-like services to clients using the SMB protocol. The `nmbd` process provides NetBIOS name server support to clients. The `SWAT` process is a self-contained Web server for administration of the Samba server. They can either be started as daemons in a start-up script such as `/etc/rc.local`, or they can be started by `inetd`. Choose only one method of starting Samba. If you chose to use `inetd`, the appropriate entries must be made manually in the `/etc/services` and `/etc/inetd.conf` files.

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

```
netbios-ns 137/udp # NETBIOS Name Service
netbios-ssn 139/tcp # NETBIOS Session Service
swat 901/tcp # Samba Web Administration Tool
```

Now, if you wish to use `inetd` to start the Samba daemons, enter suitable lines into the file `/etc/inetd.conf` in AIX 5L, such as:

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

After editing the files, type the following command:

```
# refresh -s inetd
```

Starting Samba using a script will cause the server to always be available for client requests. Therefore, starting a client connection may be slightly faster. Starting the server using `inetd` may be slower, but you will conserve system memory, and you may be able to provide additional security by using utilities such as the `tcpd` TCP wrapper. Also, if for any reason, one of these daemons dies, `inetd` would restart it automatically at the next request from a client.

### 3.2.7 Basic configuration using SWAT

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

However, sometimes it is not easy for you to configure the file itself. If you have a Web browser, try to use SWAT. SWAT is a common way to set up and maintain the `smb.conf` configuration file. It presents a simple graphical interface using your favorite Web browser. All of the pages have a similar look and feel, so it is very easy to learn to use SWAT.

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

If you set up and configured everything without errors in the previous section, you are ready to use SWAT. To start SWAT, point your favorite Web browser to the Internet address of your Samba server. You will be prompted for user ID and password, as shown in Figure 33 on page 63. You can access SWAT with any AIX user, but you can only make changes when logged in as the root user.

#### Note

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

If you make any changes to the `smb.conf` file, the Samba server will reread the file and pick up the changes every 60 seconds. The SWAT opening page is shown in Figure 34 on page 64, where you will see that there are seven categories available: Home, Globals, Shares, Printers, Status, View, and Passwords.

To open SWAT, type the host name with tcp port 901. For example, if you have installed the Samba server on AIX 5L and its host name is `rs9916d`, type the following URL:

```
http://rs9916d:901
```



You will be prompted for user ID and password, as shown in Figure 33. Log in to SWAT with root user ID and password, to configure your Samba server.

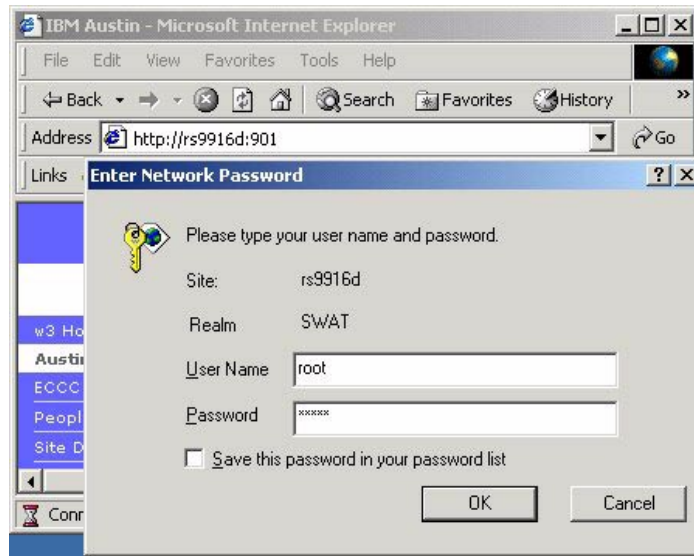


Figure 33. Enter Network Password

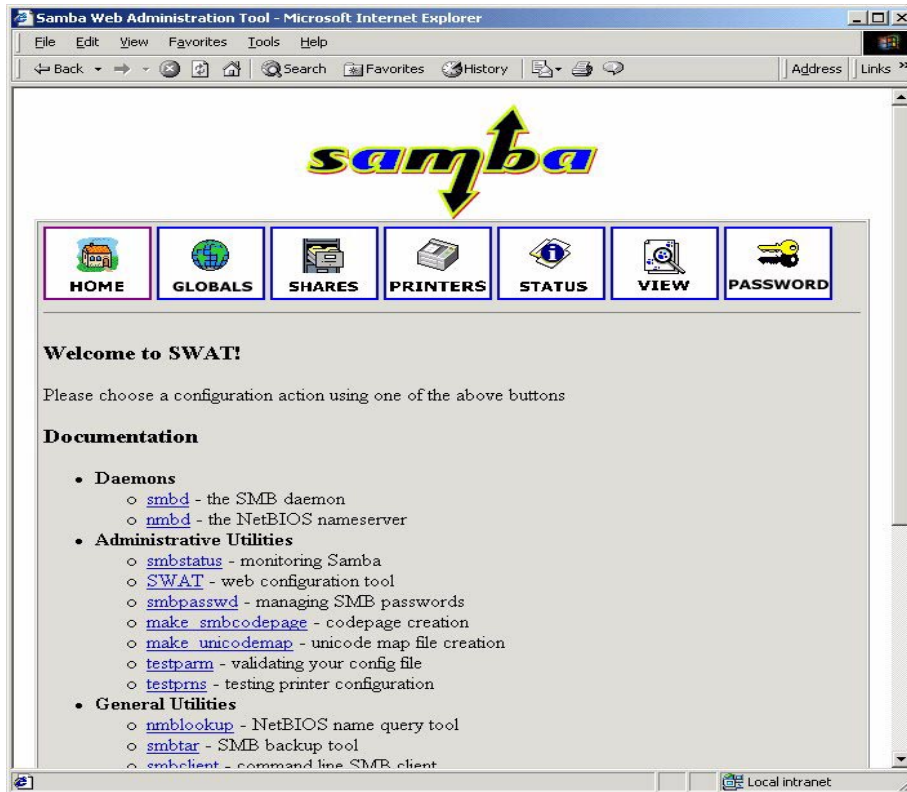


Figure 34. SWAT start page

As you can see in Figure 34, you have seven categories available:

1. Home - Here you can find all the documentation you need about Samba.
2. Globals - Here you can see and modify global parameters from the `smb.conf` configuration file.
3. Shares - Here you can view, modify, and add shares.
4. Printers - Here you can view, modify, and add printers.
5. Status - Here you can check the current status of your Samba server.
6. View - Here you can view the current configuration of the `smb.conf` configuration file.
7. Passwords - Here you can manage passwords for the Samba server.

In the following sections, we will briefly describe each of these sections.

### 3.2.7.1 Home

The Home page is the same as the start page. From here, you can go to any other section. Also, this page contains links to much of the documentation that comes with Samba.

### 3.2.7.2 Globals

When you click the **Globals** icon in the main SWAT panel, you will see a panel similar to that shown in Figure 35.

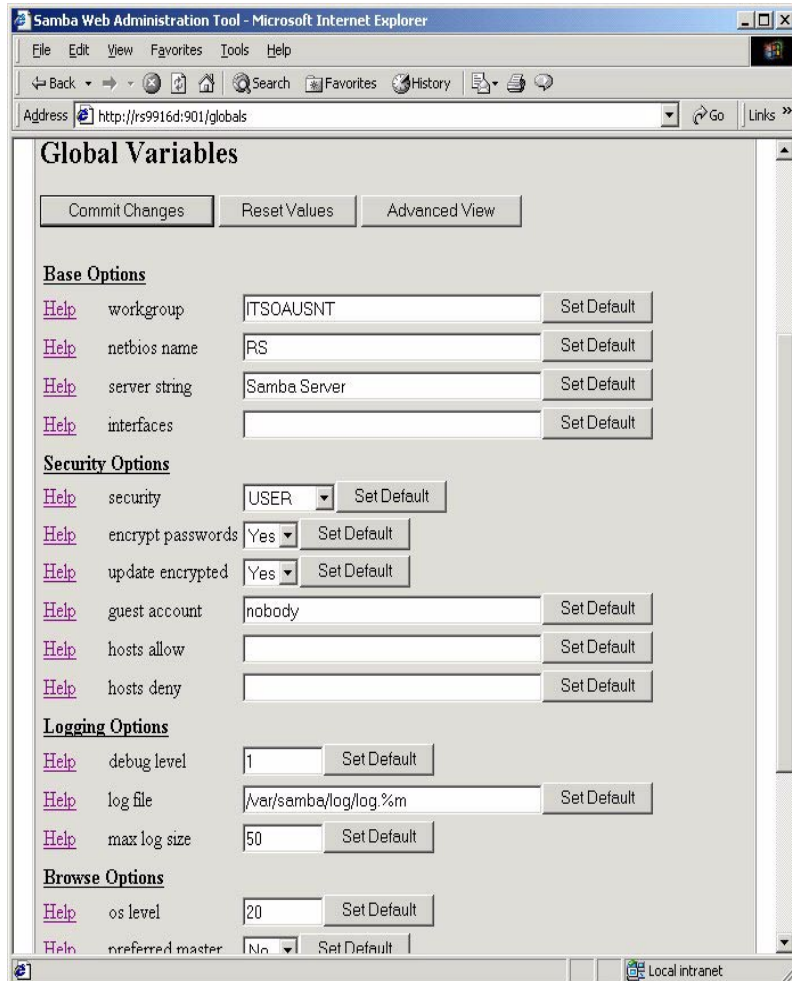


Figure 35. Global section in SWAT

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

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

Table 10 shows the parameters you might often change in the Global section.

Table 10. Parameters in the Global section

Parameter	Description
workgroup	This parameter specifies in which Windows 2000 domain or workgroup the Samba server will participate. It is equivalent to the Windows 2000 domain or workgroup name.
netbios name	This is the name by which the Samba server is known on the network. This parameter has the same meaning as the Windows 2000 Computer Name. If you do not specify it, it will default to the server's hostname.
server string	This is the description string of the Samba server. It has the same role as the Windows 2000 Description field.
encrypt passwords	Setting this parameter to yes will enable Samba to use the encrypted password protocol when authenticating users. Most newer clients (Windows NT post Service Pack 3, Windows 98, and so on) default to using encrypted passwords.
wins support	Setting this parameter to yes allows Samba to become a NetBIOS Name Server (NBNS). If you already have a WINS server on your network, set this to no and set the WINS server parameter.

### 3.2.7.3 Shares

When you open the Shares icon on any SWAT Web page, you can view a defined share, delete a share, or create a new share.

To view a share, select the share from the drop-down menu and click the Choose Share button. You will see a panel similar to that shown in Figure 36 on page 67.

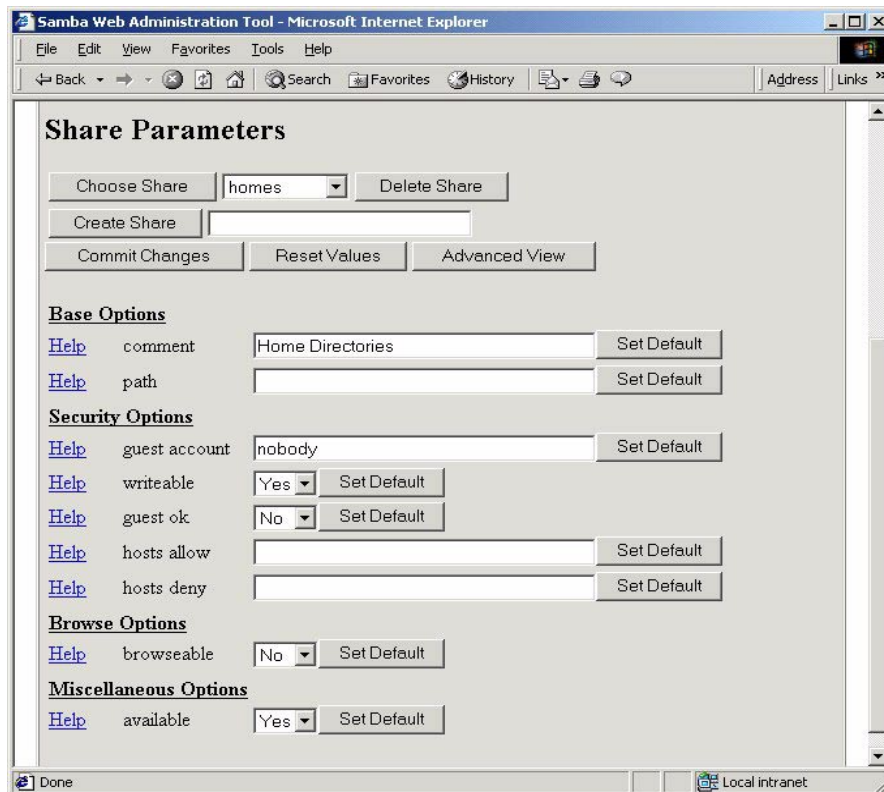


Figure 36. Shares section in SWAT

To create a new share, the directory that will be shared must exist on the server. If it does not, use the `mkdir` command to create it. Type a name for the share you want to create, and click the **Create Share** button. Now you will see a panel similar to that shown in Figure 36. Edit the new share as you would any other share; to save the new share, click **Commit Change** when you are done.

#### 3.2.7.4 Printers

In the printer section, you can view, modify, and add printers. The operations for handling printers are the same as for handling shares. You can access the printer settings by clicking the **Printers** icon on the SWAT Web page, as shown in Figure 37 on page 68.

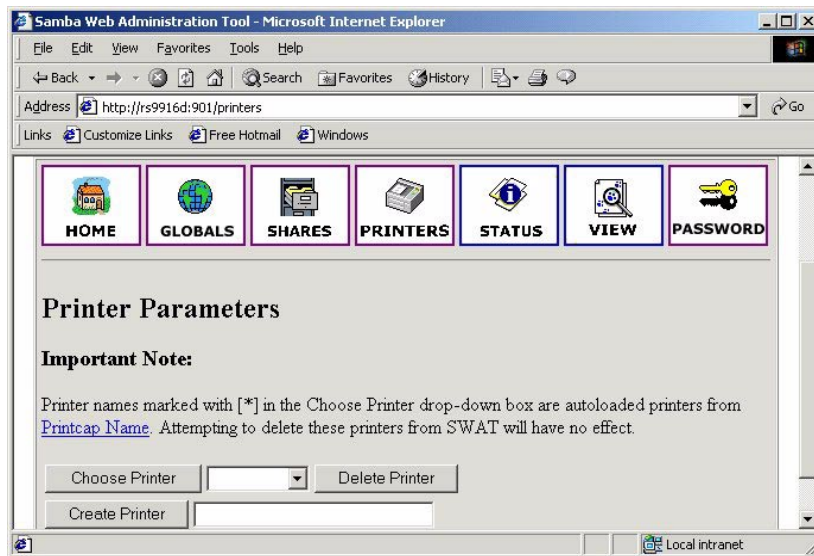


Figure 37. Printers section in SWAT

If you want to see the setting for a specific printer, select the printer from the list, as shown in Figure 38.

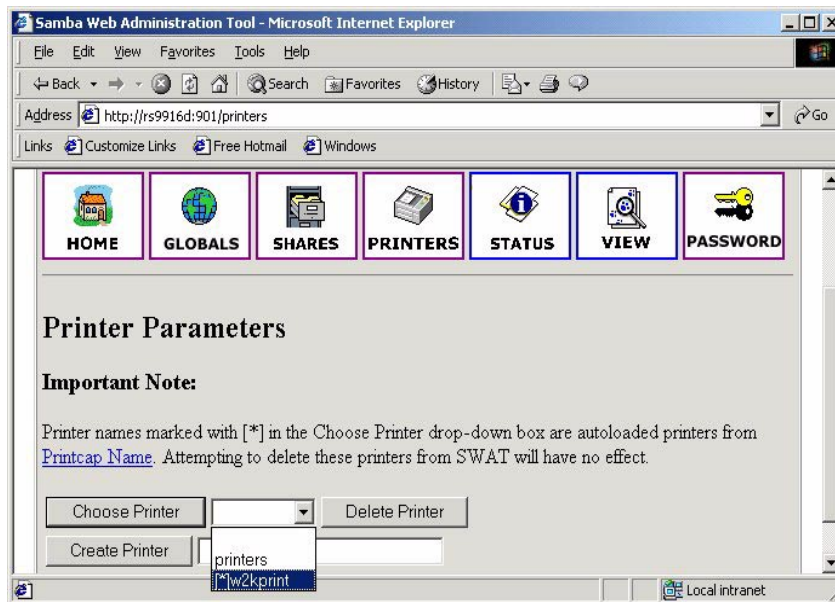


Figure 38. Selecting printer

After you have selected the printer, click **Choose Printer** to view its properties. You will see a panel similar to Figure 39.

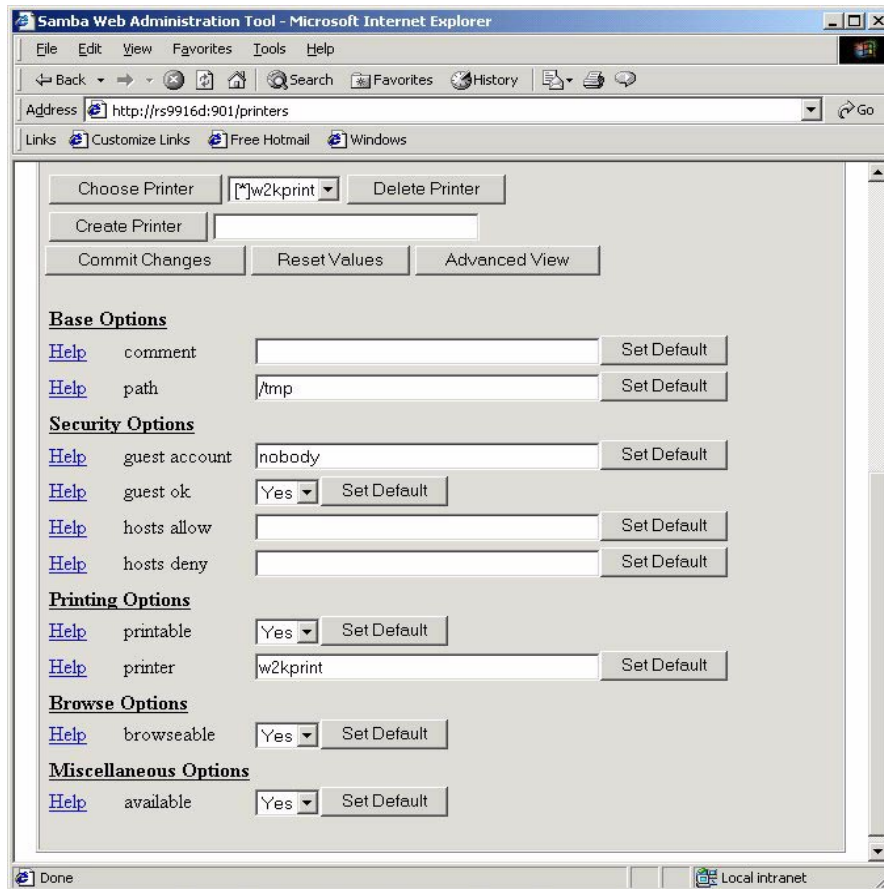


Figure 39. Printer properties

In the panel shown in Figure 39, you can modify the printer properties. When you are done, save the settings by clicking **Commit Changes**.

### 3.2.7.5 Status

In this section, you can check the status of the Samba server. Here you can see all the connections and open files. You can also start or restart the Samba server, and kill active connections (Figure 40 on page 70).

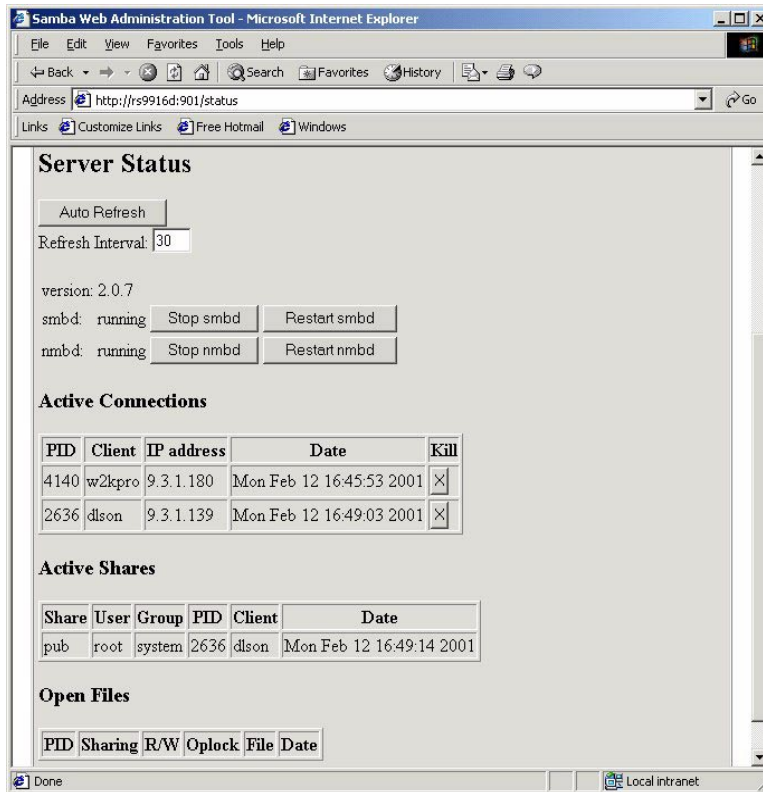


Figure 40. Status section in SWAT

### 3.2.7.6 View

In this section, you can see the current `smb.conf` configuration file. If you select **View** in SWAT, you will see the panel shown in Figure 41 on page 71. If you want to see detailed options, click the **Full View** button.



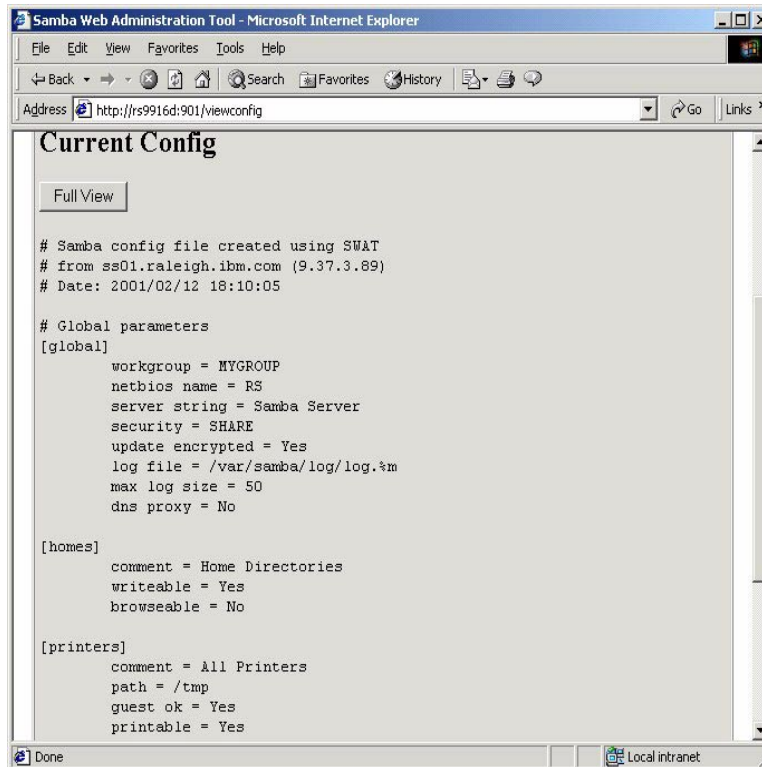


Figure 41. View section in SWAT

### 3.2.7.7 Password

In this section, you can manage the passwords of all Samba users. If you want to add a new user, put the name of user and password in *Server Password Management* and click **Add New User**. If you need to change a password for a certain user, click the **Change Password** button, as shown in Figure 42 on page 72.

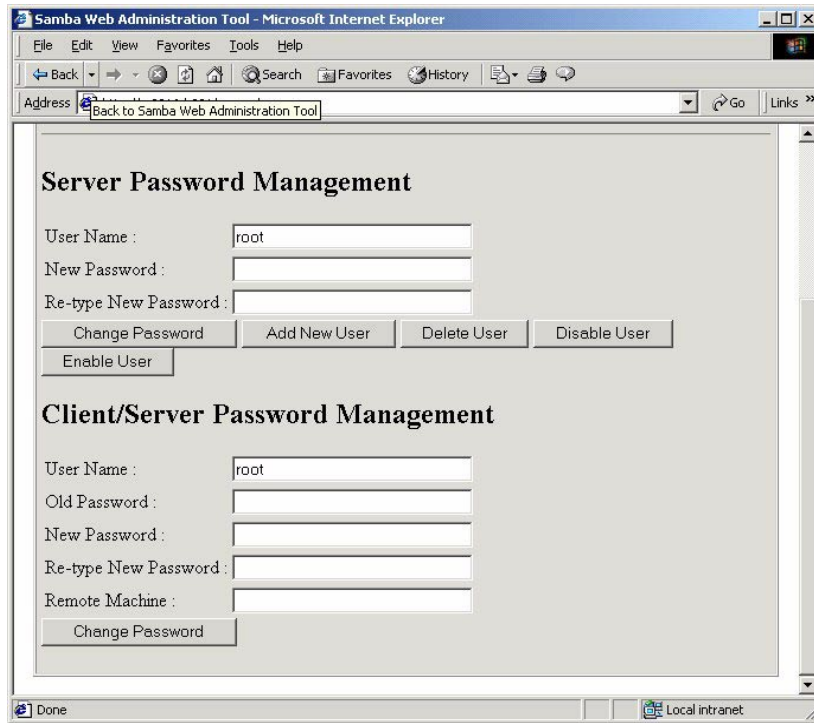


Figure 42. Password section in SWAT

### 3.2.8 Samba configuration file

You are able to configure the Samba server directly within the `smb.conf` file. Those who are familiar with the command-line mode may desire to edit the file itself. If you open `/usr/local/lib/smb.conf` with the `vi` editor, you will see the next screen:

```

[global]
    workgroup = MYGROUP
    netbios name = RS
    server string = Samba Server
    security = SHARE
    update encrypted = Yes
    username map = /usr/local/lib/user.map
    log file = /var/samba/log/log.%m
    max log size = 50
    dns proxy = No

[homes]
    comment = Home Directories
    writeable = Yes
    browseable = No

[printers]
    comment = All Printers

```

### Global parameters

The smb.conf file begins with global settings for the Samba server. If you add or change a specific parameter, the smb.conf file will look different:

```

[global]
    workgroup = MYGROUP
    netbios name = RS
    server string = Samba Server

```

For the description of some of the parameters, refer to the Table 10 on page 66.

### Share parameters

After the global settings for the Samba server come the share parameters. Most share parameters can apply to any share. These parameters are shown in Table 11.

Table 11. Share parameters

Parameter	Description
comment	This can be any string you want, but is usually used to describe the share.
path	Defines the full path to the directory to be shared.

Parameter	Description
read only	If this is set to yes, then you will not be able to write to the share.
browseable	When set to yes, the share will be visible when browsing the network.

However, there are some parameters that only apply to printer shares. The only one we used is described in Table 12.

Table 12. Printing parameters

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

### 3.2.9 Verifying Samba is installed correctly

Once the `smb.conf` file is modified to reflect your environment, you should run the provided test program to test if the `smb.conf` file is valid. The program is `/usr/local/bin/testparm`. If this program runs without errors, you have a valid `smb.conf` file. Note that SWAT will also do some basic error checking. Enter the following entry on the command line to perform the test:

```
# /usr/local/bin/testparm
```

The following screen contains an example of the output of the `testparm` program.

```
# testpam
Load smb config files from /usr/local/lib/smb.conf
Processing section "[homes]"
Processing section "[printers]"
Processing section "[tmp]"
Processing section "[pub]"
Processing section "[bmtest]"
Processing section "[s1]"
Loaded services file OK.
Press enter to see a dump of your service definitions

# Global parameters
[global]
    coding system =
    client code page = 850
    workgroup = MYGROUP
    netbios name = RS
    netbios aliases =
    netbios scope =
    server string = Samba Server
    interfaces =
    bind interfaces only = No
    security = SHARE
    encrypt passwords = No
```

### 3.2.10 Checking your server

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

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

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

The following screen shows the result of the `smbclient -L` command on our server, `rs9916d`. We see the domain, the operating system, the version of Samba being run, and the devices that have been set up to be shared with clients.

```
# /usr/local/bin/smbclient -L rs9916d
added interface ip=9.3.240.67 bcast=9.3.240.255 nmask=255.255.255.0
Password:
Domain= [MYGROUP] OS= [Unix] Server= [Samba 2.0.7]
```

Sharename	Type	Comment
printers	Printer	All Printers
tmp	Disk	Temporary file space
IPC\$	IPC	IPC Service (Samba Server)
w2kprint	Printer	
root	Disk	Home Directories

Server	Comment
RS	Samba Server

Workgroup	Master
007	KR036324
AHLENWG	WIN2KAHLEN
HAITEC	HAIPW
ITSOAUSNT	ITSONT03

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

### 3.2.11 Accessing the share resources from the client

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

#### 3.2.11.1 Configuring Windows 2000

Before you start to configure Windows 2000, make sure that you are logged on as Administrator or at least with a user who is a member of local Administrators group. Perform the following steps:

1. Right-click on **My Computer** on your desktop. The System Properties dialog box should appear.
2. Select the **Network Identification** tab, and click the **Properties** button. You should see a dialog box, as shown in Figure 43 on page 77.

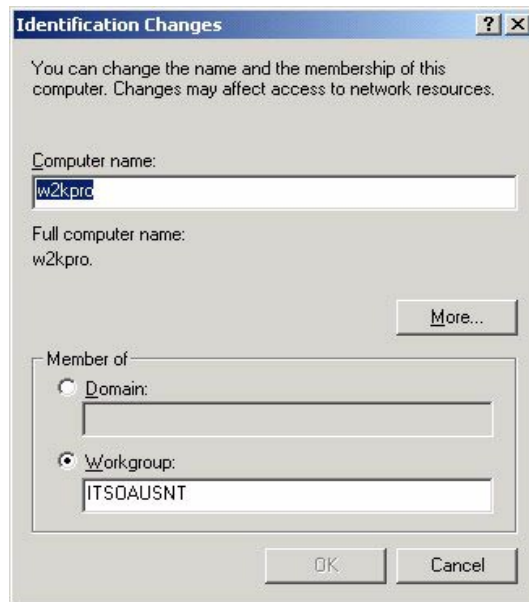


Figure 43. Identification Changes

3. Enter your computer name. Next, you have to click the radio button for **Workgroup** and enter the workgroup name.
4. Click **OK** to complete this process. Your computer will ask you to reboot. You do not need to reboot now. You can reboot when you finish the setup.
5. Right-click on **My Network Places** on your desktop. You should see the dialog box shown in Figure 44 on page 78.

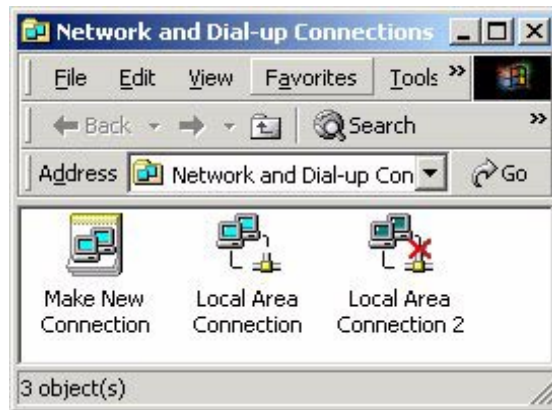


Figure 44. Local Area Connection status

6. Right-click one of your adapters and choose **Properties**, then select **Internet Protocol (TCP/IP)** and click **Properties**. You should see the Internet Protocol (TCP/IP) Properties box dialog box, as shown in Figure 45 on page 79.



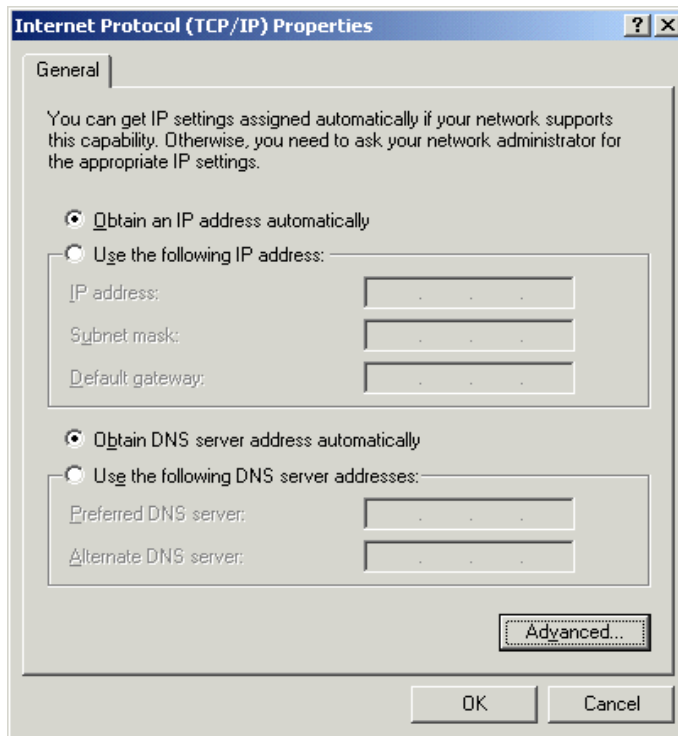


Figure 45. Internet Protocol (TCP/IP) Properties

7. Click the **Advanced** button. You should see the Advanced TCP/IP Settings dialog box. Then select the **WINS** tab. The panel shown in Figure 46 on page 80 appears.

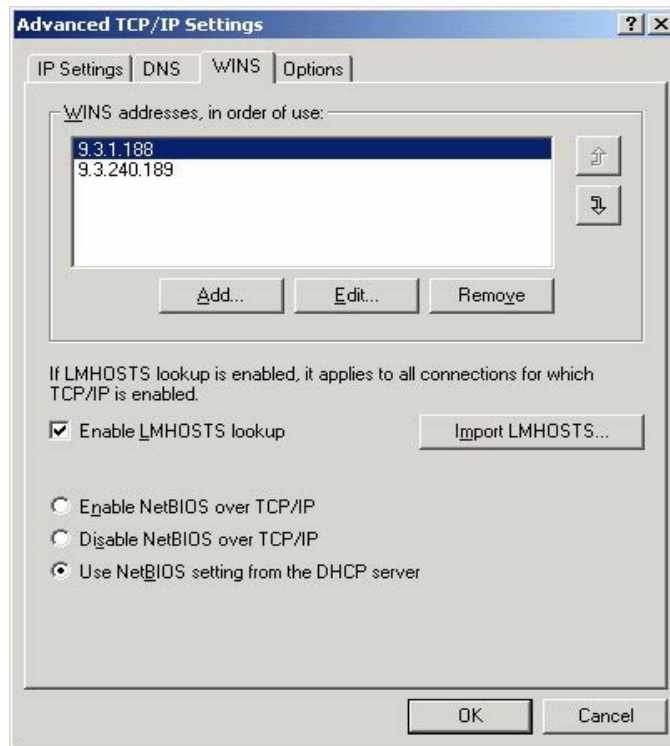


Figure 46. Advanced TCP/IP Settings

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

### 3.2.11.2 Locating the Samba server

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

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

In this section, we use the domain name and the NetBIOS server name (in this example, rs).

**Option 1: Locating the server with the My Network Places icon**

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

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 workgroup or domain of your Samba server.

**Option 2: Locating the server with the Search for Computer option**

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

1. Click the **My Network Places** icon.
2. Click the **Entire Network** icon.
3. Click the **Search for Computer** text.
4. Enter the computer name.
5. Click the **Search Now** button shown in Figure 47.

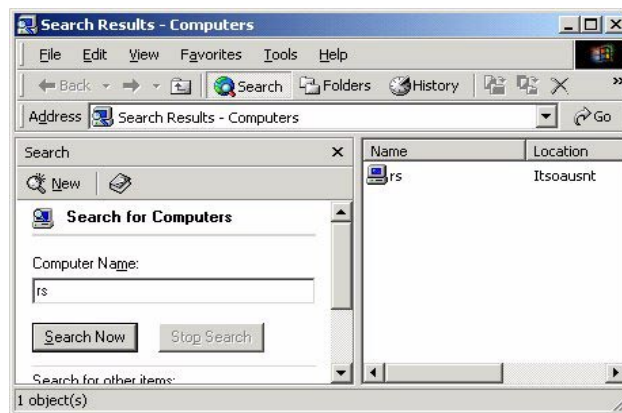


Figure 47. Search for computers

**Option 3: Locating the server from the command line**

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

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

If you use the `net view` command without command line parameters, you will 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 My Network Places. However, you cannot view a list of workgroups.

### 3.2.12 Accessing resources from the Samba server

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

#### 3.2.12.1 Accessing Files

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

##### *Option 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 perform the following steps to map a network drive to Samba shared resources:

1. Click the **My Network Places** icon.
2. Click the **Entire Network** icon.
3. Click the **Search for Computers** text.
4. Enter the computer name and click the **Search Now** button.
5. Double-click the computer name (*rs* in this example).

6. You will see the shared resources of the rs server (see Figure 48).

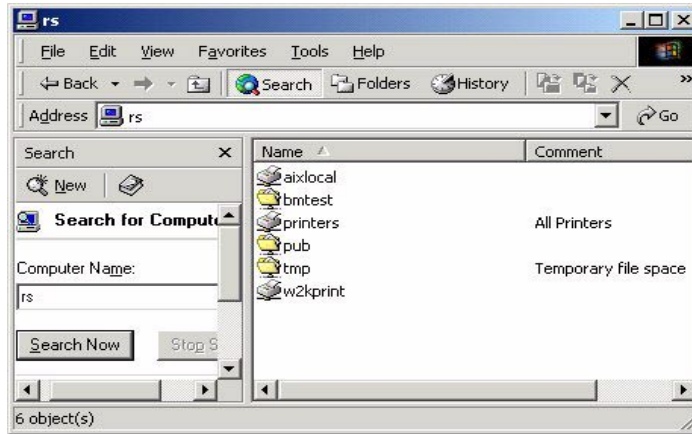


Figure 48. Samba shared resources

7. Click the shared resource (for example, tmp) and select **File -> Map Network Drive...** or right-click the shared resource and select **Map Network Drive...**
8. Select the desired drive (for example, G:).
9. Click the **Finish** button shown in Figure 49.

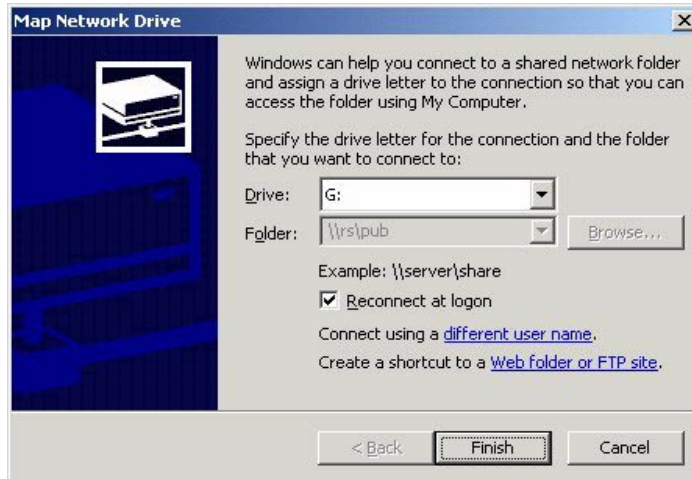


Figure 49. Map Network Drive

## Option 2: Using the command line interface

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

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

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

Status          Local          Remote          Network
-----
OK              I:             \\Itsont03\Project Data  Microsoft Windows Network
Disconnected P: \\Itsont02\Project Data  Microsoft Windows Network
The command completed successfully.
```

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

```
C:\>net use h: \\rs\pub /user:slson
The command completed successfully.

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

Status          Local          Remote          Network
-----
OK              H:             \\rs\pub        Microsoft Windows Network
OK              I:             \\Itsont03\Project Data  Microsoft Windows Network
Disconnected P: \\Itsont02\Project Data  Microsoft Windows Network
The command completed successfully.
```

You can delete network mapping with the `/delete` option as seen in the next screen.

```

C:\>net use h: /delete
h: was deleted successfully.

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

Status          Local      Remote          Network
-----
OK              I:         \\Itsont03\Project Data  Microsoft Windows Network
Disconnected P:  \\Itsont02\Project Data  Microsoft Windows Network
The command completed successfully.

```

### 3.2.12.2 Accessing printers

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

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

- GUI interface
- Command line interface

#### ***Option 1: Using the GUI interface***

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

1. Right-click on **My Network Places** and click **Search for Computers**.
2. Type the name of Samba server (in this example, rs) and click **Search Now**.
3. Select the Network printer you want to connect and double click it (in this example, aixlocal).
4. You will be prompted to install a proper printer driver in your local machine. Simply click **Yes** and **OK**.
5. Select the proper Windows printer driver (for example, select **IBM Network Printer 12 (PCL)**) from the list, and install it (see Figure 50 on page 86).

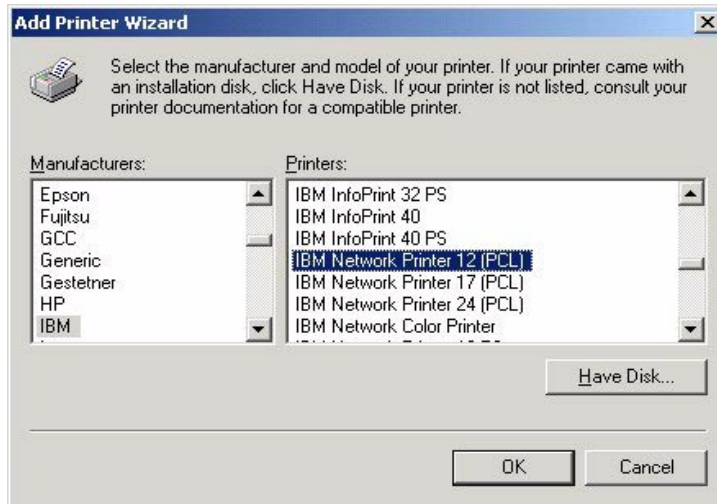


Figure 50. Add Printer Wizard

### **Option 2: Command line interface**

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

```
net use LPT1: \\rs\xaixlocal
```

### **3.2.13 Using Samba to back up a client**

Samba offers a simple solution to back up the data you have on your Windows 2000 client. The `smbtar` command is part of the standard distribution and resides in the default `/usr/local/bin` directory. It uses the standard tape archive (`tar`) format to back up the data to a file or a tape attached to the server. The following screen shows the options of the `smbtar` command.



```

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

Please enter a command line parameter!

```

As you can see, one of the elements of the `smbtar` command is the name of the share you want to back up. You then have to create a share resource on your Windows 2000 machine. To do so, select the directory you want to share, edit its properties, and select the sharing thumbnail. You should get a panel, as shown in Figure 51 on page 88. You must enter the name you want to give to this shared resource; the default is the name of the directory. Click on the **OK** button, and your directory is now accessible from the network.

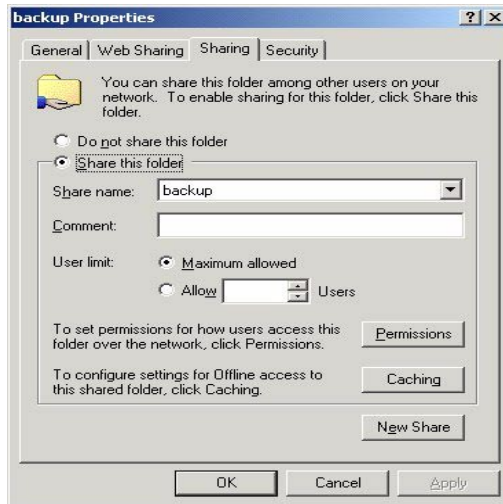


Figure 51. Sharing a directory

To check that this resource is available, use the `smbclient` command. The following example shows that the `backup` directory is ready to be backed up.

```
# smbclient -L w2kpro -U slson
added interface ip=9.3.240.67 bcast=9.3.240.255 nmask=255.255.255.0
Password:
Domain=[ITSOAUSNT] OS=[Windows 5.0] Server=[Windows 2000 IAN Manager]

      Sharename      Type      Comment
      -----      -
      E$              Disk      Default share
      IPC$            IPC        Remote IPC
      D$              Disk      Default share
      print$          Disk      Printer Drivers
      slson           Disk
      HPColor5        Printer   HPColor5
      backup          Disk
      I386Pro         Disk
      ADMIN$          Disk      Remote Admin
      C$              Disk      Default share
      w2kprint        Printer   w2kprint

      Server          Comment
      -----      -
      Workgroup       Master
```

We can now use the `smbtar` command to back up this directory. The following example shows the result of the `smbtar` command. You have to specify the name of the client with the `-s` option (in this example, `w2kpro`), the name of the share with the `-x` option (in this example, `backup`), the user used to connect to the client with the `-u` option (in this example, `slson`), and the name of the file or the tape drive you want to use for the backup (in this example, `backup.out`). You can use the `-p` option (in this example, `myahn`) on the command line to specify the password for this user on the client (in this example, `w2kpro`) machine.

```
# sbmtar -v -r -s w2kpro -u slson -p myahn -x backup -t backup.out
server    is w2kpro
share     is backup\
tar args  is
tape      is backup.out
blocksize is
added interface ip=9.3.240.67 bcast=9.3.240.255 nmask=255.255.255.0
Domain=[ITSOAUSNT] OS= [Windows 5.0] Server=[Windows 2000 LAN Manager]
restore tar file \5102ch06.fm of size 988160 bytes
restore tar file \5102TOC.fm of size 51200 bytes
tar: restored 2 files and directories
```

Once your backup is finished, you can verify the result by using the standard UNIX `tar` command, as shown below.

```
# tar -tvf backup.out
-rw-r--r--  0 0   988160 Jul 26 14:29:24 1999 ./5102ch06.fm
-rw-r--r--  0 0    51200 Jul 26 14:29:18 1999 ./5102TOC.fm
```

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

```
# sbmtar -v -r -s w2kpro -u slson -p myahn -x backup -t backup.out
server    is w2kpro
share     is backup\
tar args  is
tape      is backup.out
blocksize is
added interface ip=9.3.240.67 bcast=9.3.240.255 nmask=255.255.255.0
Domain=[ITSOAUSNT] OS= [Windows 5.0] Server=[Windows 2000 LAN Manager]
restore tar file \5102ch06.fm of size 988160 bytes
restore tar file \5102TOC.fm of size 51200 bytes
tar: restored 2 files and directories
```

If you want to back up to the tape, you can use the same command that you used to back up a file, but you need to change the `-t` parameter. Instead of the name of the file, you need to enter the tape device that you are going to use. An example is shown in the following screen.

```
# smbtar -v -s w2kpro -u slson -p myahn -x backup -t /dev/rmt0
server      is w2kpro
share       is backup\
tar args    is
tape        is /dev/rmt0
blocksize   is
added interface ip=9.3.240.67 bcast=9.3.240.255 nmask=255.255.255.0
Domain=[ITSOAUSNT] OS=[Windows 5.0] Server=[Windows 2000 LAN Manager]
 988160 ( 570.7 kb/s) \5102ch06.fm
 51200 ( 526.3 kb/s) \5102TOC.fm
tar: dumped 2 files and directories
Total bytes written: 1040384
```

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

```
# tar -tvf /dev/rmt0
-rw-r--r--  0 0   988160 Jul 26 14:29:24 1999 ./5102ch06.fm
-rw-r--r--  0 0   51200 Jul 26 14:29:18 1999 ./5102TOC.fm
```

To restore using the tape that you have attached, you can use the same command, as shown in following screen, and just modify the `-t` parameter to the tape device that you are using.

```
# smbtar -v -r -s w2kpro -u slson -p myahn -x backup -t /dev/rmt0
server      is w2kpro
share       is backup\
tar args    is
tape        is /dev/rmt0
blocksize   is
added interface ip=9.3.240.67 bcast=9.3.240.255 nmask=255.255.255.0
Domain=[ITSOAUSNT] OS=[Windows 5.0] Server=[Windows 2000 LAN Manager]
restore tar file \5102ch06.fm of size 988160 bytes
restore tar file \5102TOC.fm of size 51200 bytes
tar: restored 2 files and directories
```

### 3.2.14 Security issues

As you see in the previous sections, installing and configuring Samba server seems to be easy. However, the security issue is much more complicated. There are four security modes in Samba server, as shown in Table 13.

Table 13. Security mode in Samba server

Mode	Description
Share	With this mode, the Samba server does not check user ID. It only checks <i>password</i> for each share. This was the Samba default security level prior to Version 2.0.0.
User	This is the default SMB authentication method used by Samba 2.0.0 or later. It requires the client to present a valid username and password when connecting to the server. The name of the share that is connected to is not sent until access is granted by the server.
Server	<p>Samba 2.0.0 introduced a passthrough authentication capability to a remote SMB password server. This could either be another Samba server or a Windows server. As far as the client is aware, the server is in user-level security mode.</p> <p>The difference between <i>User</i> and <i>Server</i> mode is that you can use the Windows 2000 user ID and password for Samba connections with <i>Server</i> mode, whereas you need to create user ID and password in the Samba server you are connecting with <i>User</i> mode.</p> <p>Server-level security is useful when you want to use Windows 2000 user ID and password, and you do not have the domain controller available.</p>
Domain	<p>Samba 2.0.X introduced the ability to join an existing Windows 2000 Domain as a member server, and to trust the domain controller with the authentication process. As far as the client is aware, the server is in user-level security.</p> <p>The difference between <i>Server</i> and <i>Domain</i> mode is that the Samba server needs to join a Windows 2000 domain as a member for <i>Domain</i> mode, whereas you can use the Windows 2000 local user ID and password without joining a domain with <i>Server</i> mode.</p> <p>Domain-level security is useful when your user population does not need interactive AIX accounts. It allows you to control Samba access based on valid Domain username and password combinations.</p>

In the past, the default behavior for Samba was to authenticate users using their AIX logon and password. When the users requested access to a share, they were prompted with a panel similar to the one shown in Figure 52.



Figure 52. Request for authentication panel

Users have to enter a valid UNIX login and password on the Samba server to get access to resources. With the early version of NT 4, the logon and password are sent non-encrypted to the server. The server compares this information to the `/etc/passwd` file to determine if the logon is correct.

With Windows NT 4.0 installed with Service Pack 3, passwords are no longer sent unencrypted on the network, and the Samba server cannot immediately check them against the `/etc/passwd` file.

Note that Windows 95 OSR2 and Windows 98 also use encrypted passwords.

#### 3.2.14.1 Encrypted versus unencrypted passwords

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

Older versions of SMB clients (Windows for Workgroups, Windows 95, and Windows NT pre-Service Pack 3) send their passwords across the network as clear, unencrypted text. This allows anyone with modest technical skill to collect your password simply by running a packet sniffer on the same network segment. Recent versions of SMB clients (Windows 98, NT post-Service Pack 3, and Windows 2000) encrypt your password prior to sending it across the network.

The Samba distribution comes with instructions and registry patches to force recent clients to use unencrypted passwords.

### 3.2.14.2 Increasing the level of security on the Samba server

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

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

```
[global]
encrypted passwords = yes
```

Before you can connect from clients using encrypted passwords, you will need to create a smbpasswd file to contain the encrypted client passwords.

#### Creating a smbpasswd file

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

To create and maintain the smbpasswd file, use the command of the same name, (`smbpasswd`). The `smbpasswd` command can also be used to change SMB passwords on remote systems, including a Domain Controller.

This is an important security file and is stored in the `/var/samba/private` directory by default. It is readable only by root.

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

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

If you want add user 'myahn,' enter the following command, and you will see the screen below:

```
# /usr/local/bin/smbpasswd -a myahn
New SMB password:
Retype new SMB password:
Added user myahn.
# vi /var/samba/private/smbpasswd
myahn:224:452D3C48F26D5B2EAD3B435B51404EE:50D25107D5859707A89745E39CC625F3:[U
]:LCT-3A9548E6:
```

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

```
# smbpasswd <username>
```

The SWAT interface also allows an administrator to add and remove users and change their passwords, as shown in Figure 53.

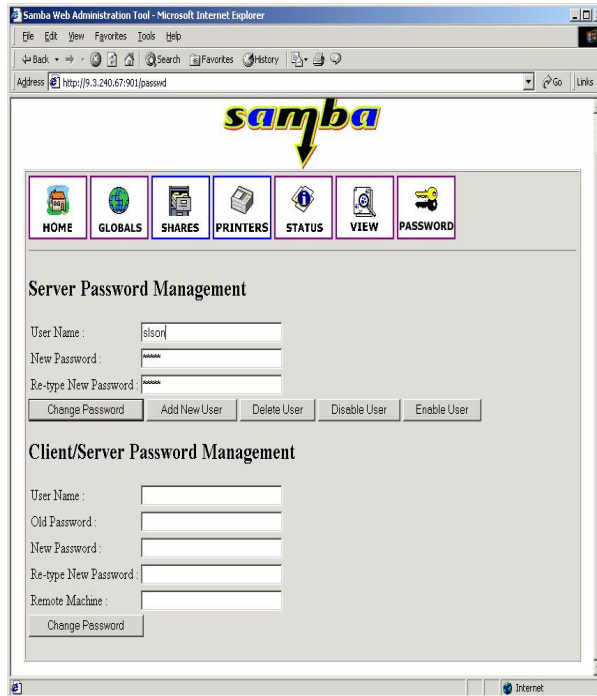


Figure 53. Password section

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

```
smb passwd file = /var/samba/private/smbpasswd
```

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

```
encrypt passwords = yes
```

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



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

Once the smbpassword file has been created, the smb password file can be maintained by using the `smbpasswd` command or the password section in the SWAT Web-based interface. SWAT allows users to be added/removed and passwords to be changed.

### 3.2.14.3 Decreasing the level of security on your Windows client

You rarely have a chance to decrease the level of security. However, if your client machines do not support encrypted password (for example, Windows for Workgroups, Windows 95, and Windows NT pre-Service Pack 3), you need to decrease the level. When the registry is changed to enable clear text passwords, it enables the Windows client to send either clear text or encrypted passwords to a server for authentication.

The level of security used for sending encrypted passwords on the network is controlled by the registry. You must be logged in as an administrator to modify security levels. To modify the registry, perform the following steps:

#### ***On Windows 2000 and NT 4.0***

1. Run **Registry Editor** (Regedt32.exe).
2. From the HKEY\_LOCAL\_MACHINE subtree, go to:
  - In Windows 2000:  
  \SYSTEM\CurrentControlSet\Services\LanmanWorkStation\Parameters
  - In Windows NT 4.0:  
  \SYSTEM\CurrentControlSet\Services\Rdr\Parameters
3. Click **Add Value** on the Edit menu.
4. Add the following lines:

```
Value Name: EnablePlainTextPassword
Data Type: REG_DWORD
Data: 1
```
5. Click on **OK**, and then quit Registry Editor.
6. Shut down and restart the machine.

Alternatively, in the Samba docs directory, use the `/usr/local/lib/samba-2.0.7/docs/Win2000_PlainPassword.reg` (NT4\_PlainPassword.reg for NT 4.0) file to patch the registry under

Windows 2000. To accomplish this, copy the file to your Windows 2000 machine and double-click it.

After the machine reboots, the passwords are sent non-encrypted over the network, and Samba works correctly.

#### ***On Windows 95/98***

In the Samba docs directory, use the Win95\_PlainPassword.reg file to patch the registry under Windows 95/98.

After the machine reboots, the passwords are sent non-encrypted over the network, and Samba works correctly.

### **3.2.15 Using a remote machine to make the authentication**

Another method you have to handle this password problem is to let someone else do the authentication of the passwords. It can be a trusted Windows 2000 server or another Samba server. There are two parameters to change in the smb.conf file to perform this operation. Use the following parameter if you are going to let someone do the authentication:

```
security = server
```

This second modification provides the Samba server with the name of the remote machine:

```
password server = w2ksrv (computer name of Windows 2000 machine)
```

Restart the Samba daemons. Now, each time the Samba server receives a request, it will forward the login and password to the remote machine to grant access to the client.

### **3.2.16 Joining an Windows 2000 domain for security authentication**

In order for a Samba Version 2 server to join an NT domain, you must first add the NetBIOS name of the Samba server to the Windows 2000 domain on the domain controller using the **Active Directory Users and Computers** menu. This creates the machine account in the domain (domain controller) Active Directory.

Assume you have a Samba Version 2 server with a NetBIOS name of RS and are joining an Windows 2000 domain called w2kdom, which has a domain controller with a NetBIOS name of w2ksrv.

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

```
smbpasswd -j w2kdom -r w2ksrv
```

We are joining the domain w2kdom and the domain controller for that domain. If this is successful, you will see the message:

```
2001/02/21 13:07:11 : change_trust_account_password: Changed password
for domain
W2KDOM.
Joined domain W2KDOM.
```

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

The filename looks like this:

```
<Windows Domain Name>.<Samba Server Name>.mac
```

The .mac suffix stands for machine account password file; so, in our example above, the file would be called W2KDOM.RS.mac.

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

Now, before restarting the Samba daemons, you must edit your smb.conf file to tell Samba it should now use domain security.

Change (or add) your Samba security mode to domain:

```
security = domain
```

Next, change the name of workgroup to your domain:

```
workgroup = w2kdom
```

This is the name of the domain we are joining.

You must also have the encrypt passwords parameter set to yes in order for your users to authenticate to the Windows 2000 domain controller.

Finally, add (or modify) the name of password server:

```
password server = w2ksrv
```

Restart your Samba daemons and get ready for clients to begin using domain security.

Let us take a look at an example of using Domain security level. Our test environment is shown in Figure 54.

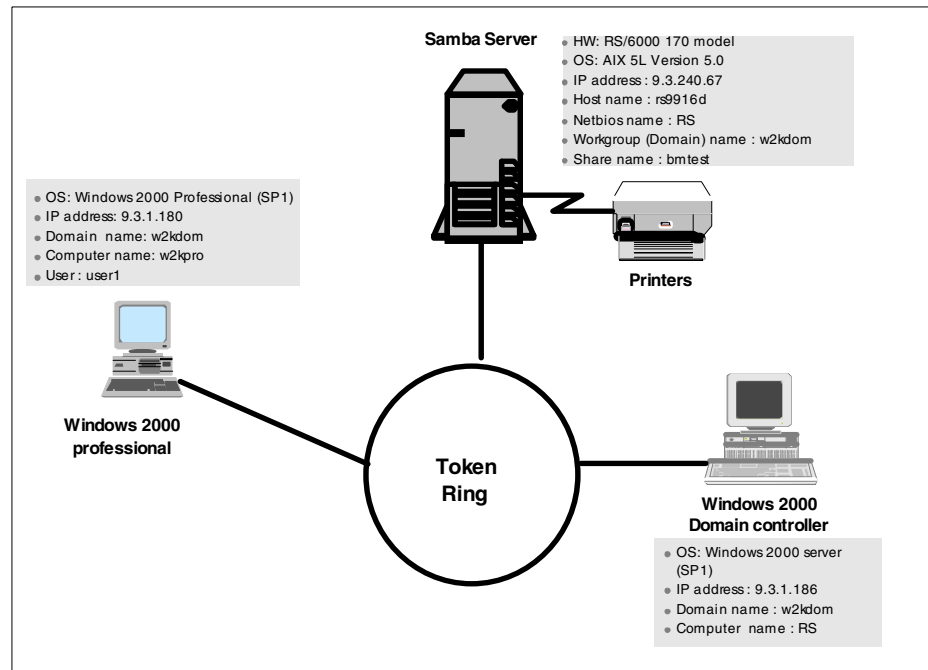


Figure 54. Example of using Domain security level

### Scenario

user1, a member of domain w2kdom is trying to connect to the Samba server from Windows 2000 Professional, in order to copy some files from the bmtest share directory. With Domain-level security, you do not need to make a smbpasswd file for user1. You can be authenticated by the Windows 2000 server domain controller.

Figure 55 on page 99 shows the required configuration of the Samba server to accomplish the above scenario.

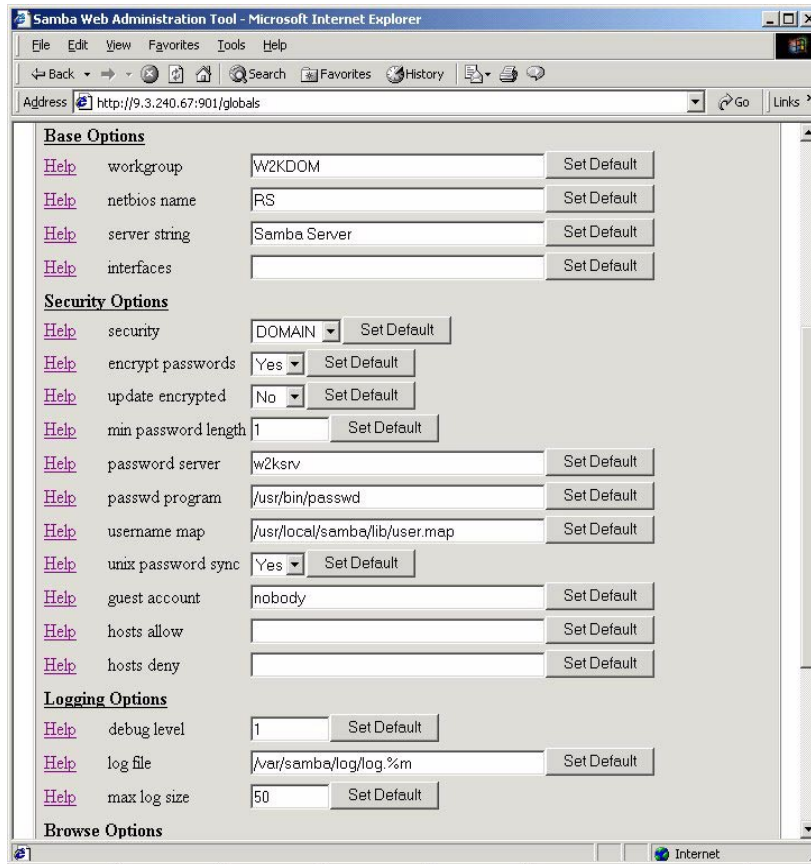


Figure 55. Configuration of Samba server

**Note**

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

### 3.2.17 Windows 2000 to AIX users mapping

It may happen that the name of your users on their client stations are not the ones they want to connect with on the Samba server. Samba provides a

mechanism that allows the mapping of Windows 2000 usernames to AIX usernames. For example, if you want users logged on the Windows 2000 client as admin or administrator to be able to log onto your Samba server as root, you just have a few steps to perform:

1. Edit the smb.conf file and add a parameter that specifies the name and location of the file that contains the correspondence between the Windows 2000 and AIX users:

```
username map = /usr/local/lib/user.map
```

2. Add a line in the /usr/local/lib/user.map file that will show that users logged as admin or administrator on the Windows 2000 machine should be logged on the AIX machine using the root user:

```
root = admin, administrator
```

3. Restart the Samba daemons.

From now on, any users logged onto a Windows 2000 system with the user admin or administrator can access the Samba server and provide the root password for authentication; the translation between the pair admin/password and root/password will be done automatically by Samba.

### **3.2.18 Windows Internet Name Service (WINS)**

In a Windows 2000 domain, you can maintain your network without WINS. However, Use of WINS (either Samba WINS or MS Windows 2000 Server WINS) is highly recommended. Every NetBIOS machine registers its name together with a name\_type value for each of several types of service it has available.

Windows Internet Name Server (WINS) is based on and compatible with the NetBIOS Name Server protocol (NBNS) and, therefore, is compatible with other implementations and Requests for Comments (RFCs). When a new NetBIOS service is made available on the network, such as a Windows machine booting or when Samba gets started, the service must be registered with the WINS server if it is to be available to clients located on other subnets.

When a machine is a WINS client, it attempts to resolve a hostname by first checking with the WINS server. If a host is not registered with a WINS server, it will attempt to find the host using a broadcast, which may be responded to by a Master Browser. If the host is still not found, “a computer or sharename could not be found” error is returned.

Samba can be used either as a WINS server that can be queried by Microsoft client, or it can be a WINS client and properly register itself with any WINS server.

Use of WINS will work correctly only if every client TCP/IP protocol stack has been configured to use the WINS server(s). Any client that has not been configured to use the WINS server will continue to use only broadcast based name registration, so WINS will not recognize it. In any case, machines that have not registered with a WINS server will fail name to address lookup attempts by other clients and will, therefore, cause workstation access errors.

**Note**

You need to set up a Samba server to point to a WINS server if you have multiple subnets and wish cross-subnet browsing to work correctly.

Samba offers WINS server capabilities. Samba does not interact with Windows 2000 server (WINS replication), so if you have a mixed Windows 2000 server and Samba server environment, it is recommended that you use the Windows 2000 server's WINS capabilities instead of Samba's WINS server capabilities.

The use of a WINS server cuts down on broadcast network traffic for NetBIOS name resolution. It has the effect of pulling all the broadcast isolated subnets together into a single NetBIOS scope across your LAN or WAN while avoiding the use of TCP/IP broadcast packets.

When you have a WINS server on your LAN, WINS clients will be able to contact the WINS server to resolve NetBIOS names. Note that only those WINS clients that have registered with the same WINS server will be visible. The WINS server can have static NetBIOS entries added to its database, but for the most part, NetBIOS names are registered dynamically.

WINS includes a method of replicating its database with other WINS servers. Samba cannot take part in such replication, but it is possible for Samba to replicate its WINS database with another Samba WINS server.

WINS also serves the purpose of forcing browse list synchronization by all Local Master Browsers (LMBs). LMBs must synchronize their browse list with the Domain Master Browser (DMB), and WINS helps the LMB identify its DMB. By definition, this will work only within a single workgroup. Note that the domain master browser has *nothing* to do with what is referred to as an MS

Windows 2000 Domain. The latter is a reference to a security environment, while the DMB refers to the master controller for browse list information only.

An alternative to WINS is to have the use broadcast over a local subnet (which would be responded to by a Local Master Browser), but this will not work across subnets. Another alternative is to use the LMHOSTS file on WINDOWS clients. The LMHOSTS file is similar to a UNIX /etc/hosts file and maps NetBIOS names to IP addresses.

For more information, see the BROWSING.txt and BROWSING-Config.txt file in the /usr/local/lib/samba-2.0.7/docs/textdocs directory.

### 3.2.19 Browsing

Viewing the resources available on a Windows network is known as browsing. The list of other hosts and domains available on a network is called the browse list. Under Windows 95/98/NT/2000, the browse list is generated to construct the view of the network in the Network Neighborhood or My Network Places. The browse list is also accessible with the `NET USE` command.

The browse list for a subnet is maintained on a computer called the *master browser*. When a new Windows computer (or Samba) starts up, it broadcasts a server announcement packet. The master browser receives this packet and adds the computer's name to the browse list. In response, the master browser transmits a list of Backup Browsers to this new computer.

With NetBIOS over TCP/IP, where Samba operates, a broadcast packet cannot reach all members of a workgroup or Windows 2000 domain that spans multiple TCP/IP subnets; one master browser must be maintained on each network segment.

To maintain a proper number of master browsers on a network, a master browser will demote itself to a backup browser and call a browser election if it receives a packet from a host claiming it should be the master browser instead.

The browser election is initiated when a computer broadcasts an election packet. An election packet will be broadcast under the following conditions:

- A browse client is unable to contact a master browser.
- A backup browser attempts to update its browse list and cannot find the master browser.
- A preferred master browser comes online.



The browser election is decided primarily on the basis of election criteria:

- Election protocol version
- Operating system type
- Time on-line
- Hostname

On a single TCP/IP subnet, the master browser has authority for the names of hosts on that subnet. Across subnets, we have to introduce the Domain Master Browser.

We need to use a WINS server whenever a cross subnet browsing is needed. If a Windows 2000 server is already a WINS server, simply use Samba as a WINS client; otherwise, set up Samba to be the WINS server. Ensure that all Windows clients are configured to use the WINS server.

For more information, see the BROWSING.txt and BROWSING-Config.txt file in the Samba docs/textdocs directory.

### 3.2.20 Troubleshooting

The Samba product seems to be very reliable and there are only a few tips needed to keep your server up and running:

- If you cannot access a shared resource, check that the daemons `nmbd` and `smbd` are running. Use the `ps -ef | grep mbd` command to check their status. If the daemons need to be restarted, the only method is to issue the `kill` command against the process ID and restart the daemons either from the `inetd` daemon or with the script that starts Samba when the server is originally started.
- Whenever a change is made to the `smb.conf` file, use the test program provided, `/usr/local/bin/testparm`, to test that you have not made any syntactic errors in the file format. Incorrect format in the `smb.conf` file can cause unexpected results once you start the Samba daemons. Another program, `/usr/local/bin/testprns`, tests for correct definition of printers in the `smb.conf` file.
- Check to ensure that TCP/IP is configured properly on both the client and the server by pinging from client to server and vice versa.
- Ensure that `smbd` is running and accessible.
- Check that the `netbios-ssn` is in LISTEN state with the command:

```
netstat -a | grep netbios
```

The output of this command is seen in the next screen.

```
# 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 -a |grep netbios
tcp4           0      0 *.netbios-      *.* LISTEN
udp4           0      0 *.netbios-      *.*
udp4           0      0 *.netbios-      *.*
```

- Ensure that nmbd is running with the command:

```
/usr/local/bin/nmblookup -B SAMBSERVER servername
```

The output of this process is seen in the following screen.

```
# ps -ef |grep nmbd
  root 13348  6192  0 10:31:35  -  0:03 nmbd
  root 14142 11628  0 14:38:44 pts/2  0:00 grep nmbd
# /usr/local/bin/nmblookup -B SAMBASERVER rs
querying rs on 0.0.0.0
9.3.240.67 rs<00>
```

- Check that the clients NetBIOS name can be resolved with the command:

```
/usr/local/bin/nmblookup -B clientname '*'
```

- Ensure that nmblookup can properly determine your broadcast address with the command:

```
/usr/local/bin/nmblookup -d 2 '*'
```

This causes nmblookup to use the default broadcast address. You will see a list of hosts on the local subnet that have responded.

- Check whether nmbd responds to a client with the command:

```
net view \\servername
```

If you get a 'network name not found' message, check whether WINS is working as expected, or create a host entry in the LMHOSTS file.

- Check whether client can connect to Samba with the command:

```
net use x: \\servername\tmp /user:myahn
```

If the NetBIOS name could be resolved in the previous step, you should be able to connect to the Samba share. If you have problems with

user/password authentication, try using the `smbclient` command to connect directly from the AIX system.

A potential problem is that when `encrypted = no` is configured, the Windows client will not authorize clear text passwords, and the Windows client must make the necessary registry change to enable clear text passwords.

- If you cannot browse the Samba server and get an invalid password error message and `encrypted = no` is configured, the Windows client will not authorize clear text passwords, and the Windows client must make the necessary registry change to enable clear text passwords.
- The Windows `nbtstat` command allows the user to query NetBIOS over TCP/IP and can be useful during problem resolution.
- Most diagnostics issued by the server are logged in a specified log file. The log file name is specified at compile time, but may be overridden on the `smbd` command line. The default log files are `/var/samba/log.smb` and `/var/samba/log.nmb`.

The number and nature of diagnostics available depends on the debug level used by the server. The server can be started with the `-d` option for `debug`. The valid `debug` level values are between 0 and 10, with 0 providing only critical error information and 10 providing the most detail. A `debug` level above 3 is intended for use by developers and generates huge amounts of very cryptic data. If you have problems, set the `debug` level to 3 and peruse the log files.

Most messages are reasonably self-explanatory. You may need to `grep` the source code for the keyword logged in the log file and inspect the conditions that gave rise to the error you observed in the log file.

The Samba Web site and the Samba distribution contain very good documentation. If necessary, refer to the man pages or the How-To pages and Frequently Asked Questions (FAQs) on the Samba Web site at:

<http://www.samba.org>

---

### 3.3 FacetWin

In this section, we will describe the connection setup between Windows 2000 and AIX using FacetWin.

We also discuss how FacetWin provides services, such as file or printer services, to a Windows 2000 client. In this case, we use AIX 5L Version 5.0 with FacetWin Version 3.1.

### 3.3.1 Overview

FacetWin brings your AIX system into your Windows network environment by providing server software that makes the resources of the AIX server available to the Windows clients on the network. The product supports Windows 95/98/Me and Windows NT 4.0/2000 environments.

#### 3.3.1.1 Features

FacetWin offers the following advanced features:

- File and Print services

The file and printer shares that you define on the AIX system appear in the PC's My Network Places just like any other Windows network resource share. File shares support file and record locking, long file names, and the Windows drag and drop interface. A printer attached to a PC can be made available to AIX applications as part of the AIX printer spooler system. File and printer sharing do not require any additional software on the client system.

- Terminal Emulation

Using this function, your character-based AIX applications can be turned into icons on the Windows desktop and menu. Double-click the icon and your application is run in a terminal emulation panel.

- Modem Server

If you install the FacetWin virtual serial port driver on a PC, then you can allow Windows applications to access the modems on the AIX server. This driver is currently only available for Window 95/98/Me.

- PC Backup/Restore

FacetWin allows one or more PCs to be backed up on a tape drive or to a disk archive on the AIX server. Users can be enabled to back up their own PCs. This backup/restore facility requires the FacetWin Agent program to be running on the PC being backed up or restored.

- E-Mail Server

FacetWin includes a POP3 mail server that can transfer e-mail from the AIX/Internet mail system to a Windows mail program such as Microsoft Outlook. The FacetWin e-mail server may be used with any mail client program that uses the POP3 protocol.

- Remote Computing

PCs connected to the AIX server via PPP are provided all FacetWin services.

- Windows Administration Tool

You can administer FacetWin either by directly editing the configuration files on the AIX server or by using the FacetWin administrator program. The FacetWin administrator is a Windows based program that organizes all of the administration details into an easy to use Windows property sheet.

- FacetWin Agent

The FacetWin Agent is a program that runs on your PC and cooperates with the backup server on the AIX server to allow a PC to be backed up. The Agent provides a “Control Panel” user interface that allows users to manage their modem server and PC backup configurations. The Agent also allows the FacetWin file and print servers to send coherent error messages to the user.

We will discuss only the file services provided by FacetWin in this book. For details on the other services, visit the following FacetCorp homepage:

<http://www.facetcorp.com>.

### **3.3.1.2 Requirements**

In order to use the complete FacetWin product, the following requirements should be satisfied.

#### ***Server Requirements***

The server requirements to use FacetWin on RS/6000 or pSeries Server are:

- AIX Version 3.2, 4.X, or AIX 5L
- 6 to 8 MB of available disk space
- TCP/IP operational
- PPP operational (in order to use FacetWin remote (dial-up) functionality)

#### ***Client Requirements***

The client requirements for FacetWin are:

- TCP/IP operational.
- 5 MB of available disk space to install additional software for terminal emulation, modem server (Windows 95/98/Me only), backup, or FacetWin Administrator functionality.

In order to use the FacetWin product, your PCs must be running one of the following operating systems:

- Windows 95
- Windows 98/Me
- Windows NT4.0
- Windows 2000
- Windows 3.1/DOS
- Citrix/Windows Terminal Server

### 3.3.1.3 FacetWin Documentation

You can get FacetWin documentation from various sources.

- The installation manual is delivered with the installation media.
- The installation instructions are provided on a CD-ROM and as a downloadable file.
- FacetWin hardcopy booklet is available after purchasing a license. The booklet, in PDF format, is on the installation media and is available at the FacetCorp Web site:

<http://www.facetcorp.com>

- After FacetWin's installation on an AIX machine, you can use the UNIX man pages by using the command:

```
# man facetwin
```

- The Windows help files provide an online version of the FacetWin manual.
- Other support documents are available from:

<http://www.facetcorp.com>

## 3.3.2 Installing the FacetWin AIX Server

The general installation plan is to install FacetWin on an AIX server first, then on a PC client, and ensure that the software is operating properly. Once this first server can use FacetWin services properly, then you can proceed to install it on the other servers and PCs. If you are only planning to use the FacetWin file and print services, you will only need to install the software on AIX.

### 3.3.2.1 Preparing AIX server

Before installing FacetWin on an AIX server, you should ensure that TCP/IP is operating properly.

If you plan to use the FacetWin remote computing features, you have to install PPP services on the AIX server. However, FacetWin can be installed and

used on the network without having PPP operational. The PPP configuration can be done at a later time, before using the remote computing features.

**Note**

If your system already has another SMB server installed, you should disable this existing SMB server. Multiple SMB servers cannot be used on a system at the same time.

### 3.3.2.2 Preparing UNIX installation notes

The following information will guide you in creating a set of notes that will be used while running the installation procedure:

- Determining the installation directory for FacetWin

The default installation directory on the AIX server is `/usr/facetwin`. However, you can customize it during the installation procedure. The FacetWin installation only uses about 6 to 8 MB of disk space, and it will increase as you add configuration information, but the amount of extra disk space needed is usually small. However, if you want to use PC backup functionality, you will need large disk spaces for archiving. The default path for the PC backup archive is a subdirectory beneath the installation directory, so you have to give a disk archive a full path name or relocate the installation directory to a larger disk partition.

- Determining the FacetWin File and Print Services Security Mode

You must decide on a security method before using FacetWin File and Print services:

#### ***NT server***

This is available to you if you have a Windows NT or Windows 2000 machine on your network that knows the Windows usernames and passwords of all of your users. This will usually be your Primary Domain Controller. If you have such a server, then the NT server is the recommended security method. Users who connect to shares on an AIX machine through FacetWin File and Print services will be authenticated by checking with the NT server that you specify. This method does not expose plain-text passwords on the network, and will work with all Windows clients without the need for any further configuration changes.

#### ***UNIX***

This method allows your users to use their AIX usernames and passwords to log in. Passwords that are changed using the standard AIX utilities will

be changed for FacetWin access. However, the UNIX security method requires plain-text passwords to be exchanged over the network.

### **LANMAN**

This method checks the password that the user entered against an encrypted password that is stored in a file called `fcpasswd` on the AIX machine. If you choose this method, you will have to enter every user's PC password into this file using the `fc_encrypt` command, and you will have to update it every time the user's Windows password changes. This method does not expose plain-text passwords on the network, and will work with all Windows clients without the need for registry changes.

### **RHOST**

It is not used very often because it requires fixed IP addresses and a clear understanding of the `$HOME/.rhost` and `/etc/hosts.equiv` files. It checks the DNS name or IP address of the workstation against these files to decide whether or not to allow access.

- Determining the Workgroup or Domain to which the AIX server will belong

During the installation steps, you will be asked to define the name of Workgroup or Domain to which the AIX server will belong. The Workgroup is a Microsoft networking concept for grouping computers together in the Network Neighborhood or My Network Places. The Domain is a security concept for authenticating users. If you already have PCs configured together on the network and you want the AIX server to appear in the Network Neighborhood or My Network Places with these PCs, you must determine what name they are already using for the Workgroup or Domain. If you have multiple Workgroups/Domains on your network, at least one PC must be in the same Workgroup/Domain as the AIX server.

To determine the name of Workgroup/Domain, follow these steps on a PC that is in the workgroup or domain that AIX server will join:

- a. From the Start button, select **Settings** -> **Control Panel** and then double-click the **System** icon.
- b. On the System properties dialog box, select the **Network Identification** tab and click the **Properties** button. You should see a dialog box, as shown in Figure 56 on page 111.



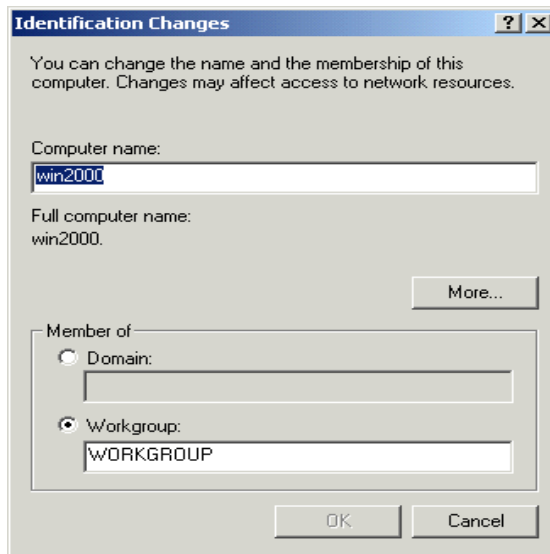


Figure 56. Getting the name of Workgroup/Domain

### 3.3.2.3 Installing FacetWin on a AIX server

There are several ways to install FacetWin on an AIX server, including from CD, diskette, and tape. In this section, we will describe the installation method from CD.

At the AIX server, perform the following steps in order to install FacetWin:

1. Login as root.
2. Create the /cdrom directory, if it does not already exist.
3. On the command line, enter the following command:  

```
# mount -rv cdrfs /dev/cd0 /cdrom  
# cd /cdrom/facetwin/aix5L-power
```
4. Run the installation procedure with the command:  

```
# sh install.sh
```
5. The installation procedure will begin. You will be prompted:

```
Before installing FacetWin for the first time, you must read
the "Preparing UNIX Installation Notes" section in the
Installation booklet, the CD help file, or the install.txt
file. This will explain how to choose a security mode.
```

```
Have you prepared the UNIX installation notes as described in
the installation instructions [Y/N] (default N)?
```

You should have the notes that you prepared in the previous section. If you do not, answer N and the installation procedure will exit.

If you answer Y, you will be prompted with:

```
Checking FacetWin software installation files.
Checking for FacetWin servers already running.
Specify destination directory [press ENTER for default /usr/facetwin]:/facet
```

Press Enter to accept the default, or define an alternate FacetWin installation directory. In this example, we chose /facet directory.

The next prompt will be:

```
=====
Fri Feb 9 11:42:50 CST 2001
Preparing to install FacetWin software in /facet.
Which security method do you want to use for file and print services?
  Enter 1 for NT SERVER
      2 for UNIX
      3 for LANMAN
      4 for RHOST
Select Method [1-4] (or "Q" to quit):3
```

Select the method that you have chosen. In this example, we chose 3.

The next prompt will be:

```
pass_security=LANMAN
Enter name of the workgroup or domain that should include this machine
(or QUIT to quit):workgroup
```

In this step, you should input the name of workgroup or domain. In this example, we defined its name as workgroup.

The installation procedure will continue with no further interaction. The output is shown in the next screen.

```
workgroup=workgroup
Installing FacetWin software.
10754 blocks
Setting up default configuration.
Running fct_encrypt -b to create fctpasswd file.
Updating /etc/services and /etc/inetd.conf files
Adding POP3 server (fct_pop3d) to inetd.conf file
Adding session server (fct_nbsd) to inetd.conf file
Refreshing inetd
0513-095 The request for subsystem refresh was completed successfully.
Installing links to programs. (The message '0 Blocks' is normal.)
1398 blocks
Links installed.
Installing FacetWin man pages. (The message '0 Blocks' is normal.)
150 blocks
61 blocks
274 blocks
100 blocks
Man pages installed.
Start FACETWIN LICENSE server
Start FACETWIN WINS server
Start FACETWIN BROWSER server
All FacetWin servers started.
Installation is done
Fri Feb 9 13:09:29 CST 2001
```

If your system already has another POP3 server installed, you will be asked if you want to replace it with the FacetWin POP3 server.

6. After the installation procedure is finished, the FacetWin server software should be completed. The installation procedure will log all of its output to a file named log.txt, which is in the FacetWin installation directory (in this example, /facet). It is a good idea to inspect this file to be sure that there were no error messages that you missed on the screen output.

#### 3.3.2.4 Preparing Windows 2000 for FacetWin

Before you can use FacetWin with a PC running Windows 2000, you must have the Windows network system configured properly. The following components are required:

- Client for Microsoft Networks
- Internet protocol (TCP/IP)
- File and printer sharing for Microsoft Networks

Make sure these components are installed and operating properly.

### 3.3.3 Accessing FacetWin server from Windows 2000

Depending on the security method you chose, you have to do some additional configuration before your PC can access file and printer shares on the AIX server. In this book, we will discuss the LANMAN security method, which does not need an NT server or plain-text password. In case you chose another security method, see the FacetWin manual delivered with the FacetWin installation CD.

The LANMAN security method requires that the user's DES encrypted passwords be kept up to date in the `fctpasswd` file. This file is in the FacetWin installation directory on the AIX server (`/usr/facetwin` by default, `/facet` in this example). The installation procedure will have built an initial `fctpasswd` file with usernames but no passwords. The passwords must be added using the `fc_encrypt` command with the AIX username on the AIX server, as follows.

```
# fc_encrypt ausres21
Changing password for "ausres21"
ausres21's New Password:
Re-enter Password:
```

For information about this program, run the following command on the AIX server:

```
# man fc_encrypt
```

Once you have completed any of these configuration steps that apply to your situation, then you are ready to test access to shares on the AIX server.

#### 3.3.3.1 Locating FacetWin server

To locate FacetWin server on Windows 2000 client machine, do the following:

1. Click the **My Network Places** icon.
2. Click the **Entire Network** icon.
3. Click the **Computers Near Me** icon.

You will see the FacetWin server, as seen in Figure 57 on page 115. If the AIX server fails to appear, try using the Search button on the toolbar.

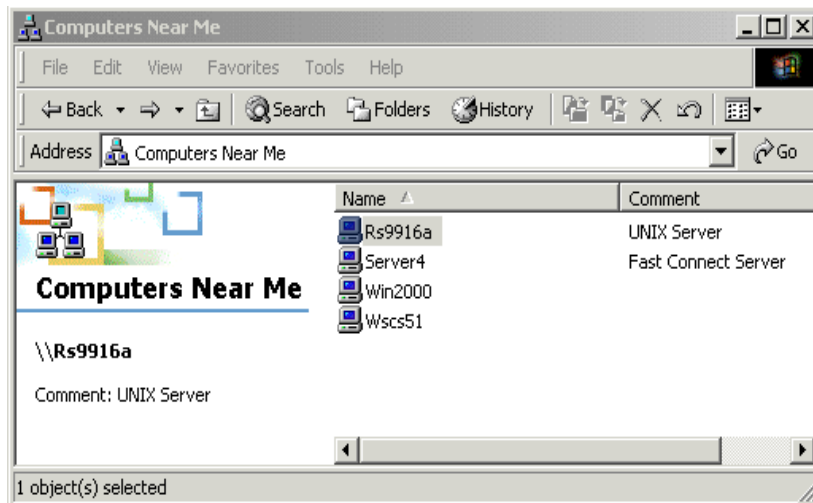


Figure 57. Locating FacetWin server

### 3.3.3.2 Accessing resources from FacetWin server

To access FacetWin server on Windows 2000 client, just click the server name in Figure 57. You will see the exported file shares by default, as in Figure 58.

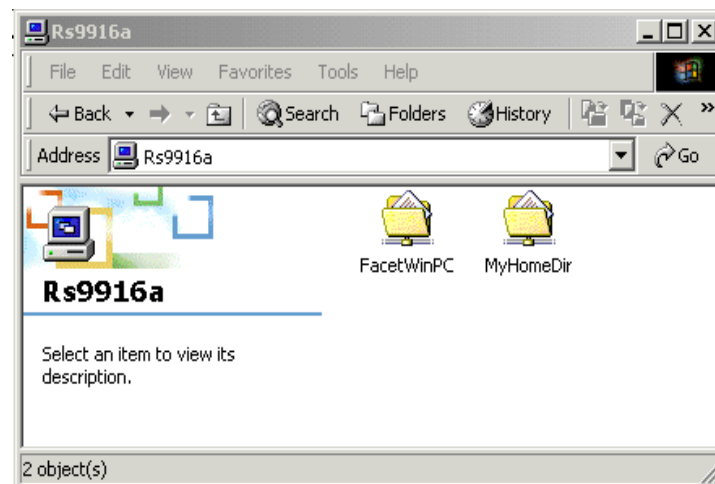


Figure 58. Accessing file shares on FacetWin server

### 3.3.4 Installing FacetWin on a PC

FacetWin PC software can be installed from the FacetWin CD, or from an AIX server that has FacetWin installed and is sharing files properly with the PC.

In this section, we will explain the installation procedure of FacetWin on a PC from the AIX server.

In order to install from the AIX server, you must have successfully gained access to the file and printer shares on the AIX server, as described in Section 3.3.3, “Accessing FacetWin server from Windows 2000” on page 114.

If you can access the exported file share, proceed with the next step:

1. On your PC, double-click on the **My Network Places** icon, and then double-click the **Computers Near Me** icon.
2. Find the AIX server that FacetWin has been installed on, and double-click on its icon. The shares that are currently defined on the server will be displayed (Figure 58 on page 115). One of the shares will be named ‘FacetWinPC.’ Double click on this icon and the contents of that share will be displayed (Figure 59).

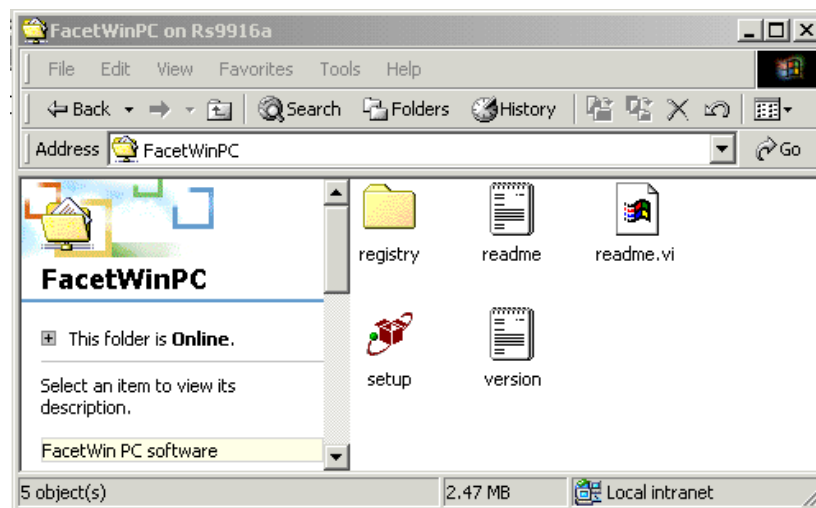


Figure 59. Installing FacetWin on a client from a server

3. Double-click on the setup item. The installation will begin on the PC. Follow the instructions on the panel to complete the installation. For

administering FacetWin on a client, you should check the box of the 'FacetWin Administrator' item, as shown in Figure 60.

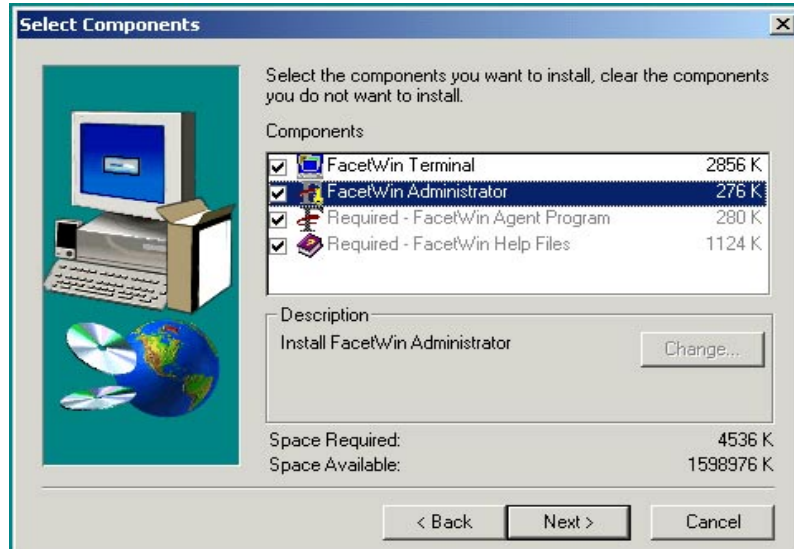


Figure 60. Select Components

4. After the PC software has been installed, a 'FacetWin' group will have been added to the Windows start menu.
5. If you installed everything, the following items will have been added:
  - The "Add a UNIX Application" item is used to create and configure a new FacetWin terminal emulator configuration to run an application on a UNIX server.
  - The "FacetWin Administrator" item will run the Windows-based administration program and provide context sensitive help. If you run this program, you get a GUI interface, as seen in Figure 61 on page 118. Using this interface, you can define file and print shares, PC Backup, Name services, Security method, and other configurable parameters on the client side.

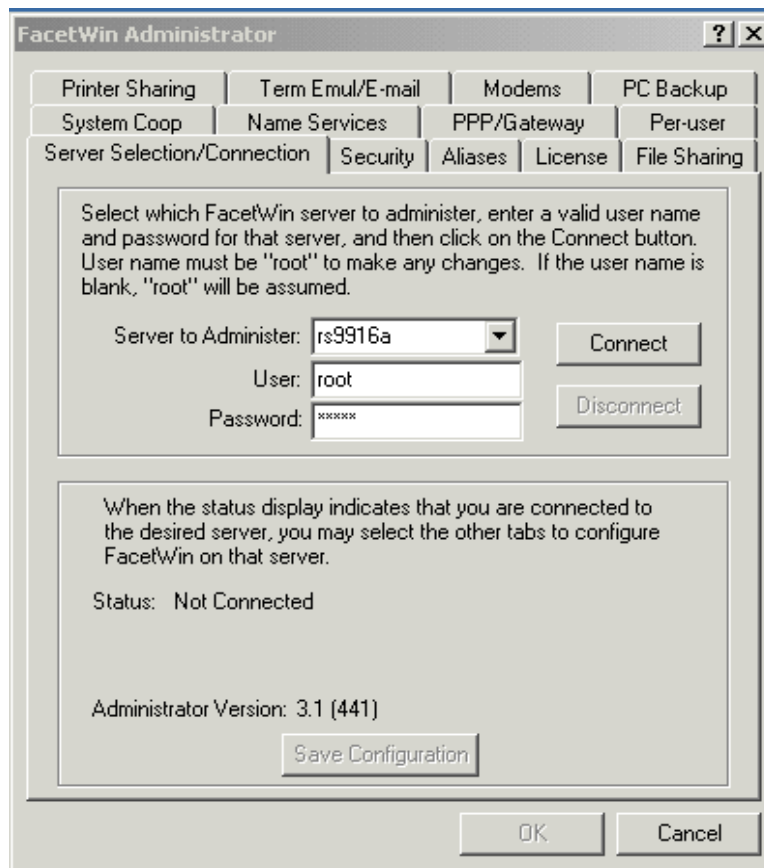


Figure 61. FacetWin Administrator

- The “FacetWin Agent Control Panel” item will run the configuration program that allows users to configure user definable FacetWin features on their PC (Figure 62 on page 119).



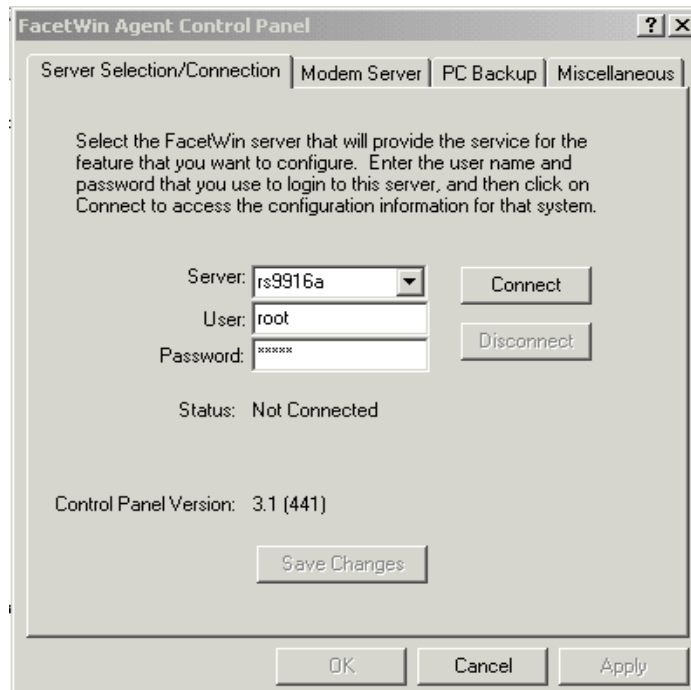


Figure 62. FacetWin Agent Control Panel

- The “FacetWin Agent” item will run the agent program that must be running to back up the PC or display enhanced messages from the FacetWin servers.
- The “FacetWin Help” item will open a help panel that displays the contents of the FacetWin help file. The entire FacetWin product is documented in this help file.
- The “FacetWin Terminal Configurations” item will open an Explorer panel in the folder where all the configurations are kept. You can right-click on the configurations displayed there in order to change their properties. You can double-click a configuration to start the UNIX application it describes.
- The “FacetWin Uninstall” item is used to remove the FacetWin PC software. There is no need to run this item when upgrading FacetWin software; run this item only when removing FacetWin from the PC permanently.

### 3.3.5 File sharing

The *File Sharing* tab of the FacetWin Administrator is used to manage the file shares on the server.

If you click the File Sharing tab, you will see the panel shown in Figure 63.

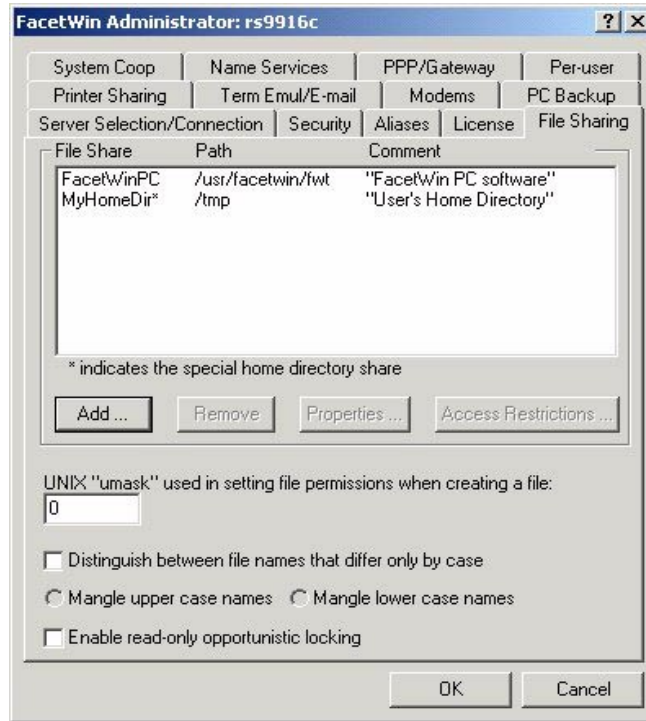


Figure 63. File Sharing tab

To add a new share, click **Add** and give the **Share Name** and **Share Path**, as shown in Figure 64 on page 121.

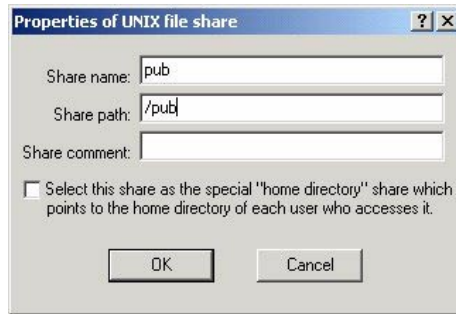


Figure 64. Properties of UNIX file share

When you have completed adding a new share, users can connect to the share from My Network Places (Network Neighborhood).

When you add a new share, you might be prompted with the information that the *Special Home Directory Share* will be changed. This box should only be checked for the *My Home Directory Share*, or a share that you choose to replace it.

Special Home Directory Share is designated as the special home directory share (if any) that will have an asterisk after its share name. The home directory share is a special share that points to the home directory of each user who accesses the share. So, rather than pointing to a fixed directory as regular shares do, it points to a different directory for each user. A user's home directory is specified in the `/etc/passwd` file and is exported to the `$HOME` environment variable. There can only be one special home directory share on each FacetWin server. By default, a share named *MyHomeDir* will be the special home directory share.

### 3.3.6 Print sharing

The *Print Sharing* tab of the FacetWin Administrator is used to manage the print shares on the server.

If you select the Print Sharing tab and click **Add**, you can see the panel shown in Figure 65 on page 122. Give the name of the share, the temp directory in AIX, and the script. Figure 65 on page 122 shows us the typical use of script for printing.

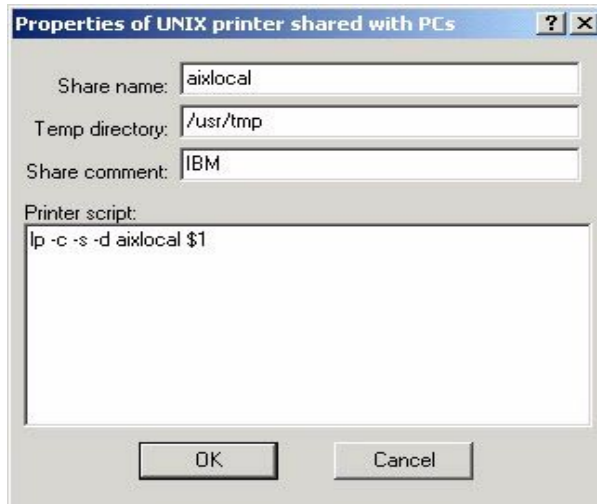


Figure 65. Properties of UNIX print shared with PCs

When you are done adding a print share in the FacetWin Administrator, you need to add a new network printer with My Network Places or the Add Printer Wizard in the control panel.

You can perform the following steps to add a network printer with My Network Places:

1. Right-click on **My Network Places** and click **Search for Computers**.
2. Type the name of FacetWin server (for example, rs9916d) and click **Search Now**.
3. Select the Network printer you want to connect and double-click it (for example, aixlocal).
4. You will be prompted to install the proper printer driver in your local machine. Simply enter Yes and click **OK**.
5. Select the proper Windows (such as **IBM Network Printer 12 (PCL)**), printer driver from the list, and install it (see Figure 66 on page 123).

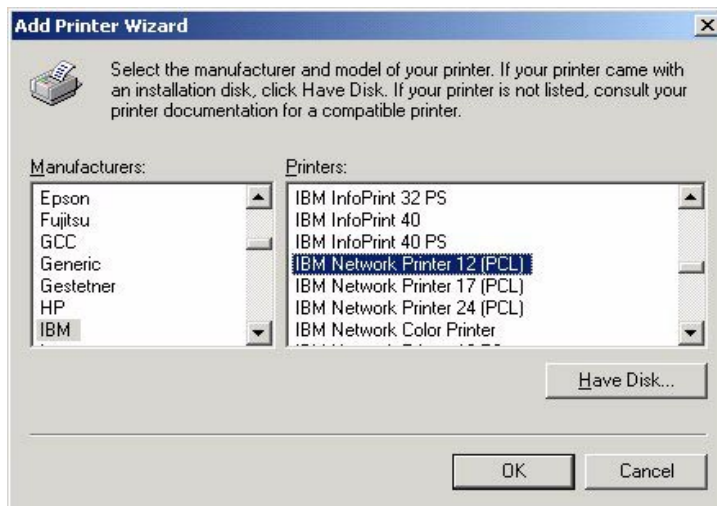


Figure 66. Add Printer Wizard

### 3.3.7 FacetWin UNIX commands

This section will describe how to administer FacetWin using FacetWin UNIX commands on AIX server.

You can use following commands for FacetWin server administration and troubleshooting on the server side.

- Using the `fct_admin` command, you can perform basic administration jobs like starting/stopping FacetWin servers, managing licenses, and sending a message to clients. The screen below shows the initial menu of the `fct_admin` command.

```

*----- FacetWin Administration Menu -----*

1. Show FacetWin license information.
2. Edit FacetWin licenses (must be root).
3. Start FacetWin Servers (must be root).
4. Stop FacetWin Servers (must be root).

5. FacetWin WINS Server Status.

6. Show FacetWin version information.

7. Send message to FacetWin user(s).

Q. Quit

*-----*
Enter number and press RETURN or Q and press RETURN:

```

- The `fct_licinfo` command shows the status of FacetWin License Server as shown in the next screen.

```

# fct_licinfo
Contacting FacetWin License Server...
Connecting to FacetWin License Server...

*****
FacetWin License Information (v3)                Mon Feb 12 15:34:05 2001
*****

License Server:  9.3.240.51  rs9916a
Started:        Mon Feb 12 14:07:43 2001
Machine ID:     rs6-yqck4bs5-x

License type:   Demo
License version: 3
Expiration:    11 Mar 2001  (See fct_licedit for details)
Licensed users: 50
Current users:  0

-----

License Summary

License version: 3
Licensed users:  50
Current users:   0

```

- The `ps -ef | grep facetwin` command shows the status of the FacetWin process.

- FacetWin processes report informational, warning, and error messages in the syslog file when \*.debug is enabled.





## Chapter 4. Services for UNIX Version 2.0

This chapter will discuss the Microsoft Services for UNIX (SFU) Version 2.0. Even though the product does support Windows NT 4.0, the scope of this book only covers Windows 2000.

SFU provides a set of additional features to Windows 2000 that allow for greater interoperability with existing UNIX-based systems, for example, AIX. In addition to a whole range of interoperability components, SFU also leverages existing UNIX network resources in simplifying network administration and account management across both platforms.

### 4.1 System requirements

To successfully install and run SFU, the minimum system requirements are:

- 60 MB of available hard disk space for a full installation
- 16 MB of RAM (on top of your current memory configuration)
- One network adapter (Ethernet, Token Ring, or FDDI)

**Note**

SFU currently does not support clustered systems.

Table 14 shows the different components of SFU and what version of Windows 2000 they support.

Table 14. Microsoft Services for UNIX Version 2.0 component availability

Component	Required Operating System	
	Windows 2000 Professional	Windows 2000 Server
Client for NFS	X	X
Server for NFS	X	X
Gateway for NFS		X
Server for PCNFS	X	X
Server for NIS		X
User Name Mapping	X	X
Password Synchronization		X

Component	Required Operating System	
	Windows 2000 Professional	Windows 2000 Server
Telnet Client	X	X
Telnet Server	X	X
Server for NFS Authentication	X	X
Remote Shell Service	X	X
CRON Service	X	X
ActivePerl	X	X
UNIX Shell and Utilities	X	X

Additional requirements and caveats:

- Client for NFS and Gateway for NFS *cannot* co-exist on the same physical machine.
- Server for NFS can authenticate users using local server accounts or Windows domain accounts. If users are to be authenticated using local accounts, Server for NFS Authentication must be installed on the same server as Server for NFS. If users are to be authenticated using domain accounts, Server for NFS Authentication must be installed on all Domain Controllers (DCs) in the domain, because there is no way of knowing which DC will authenticate the user at any given time.
- For domain passwords, Password Synchronization must be installed on a server serving as a DC.
- The server for NIS must be installed on a DC.
- Make sure that the installation directory does not include a space in its name. Otherwise, some shortcuts will not work correctly. In addition, you might experience problems with NFS, and some UNIX utilities and scripts.
- When you install SFU, the system's command path is modified to place the %SFUDIR%\common directory before other directories. As a result, the SFU `find` command will be run instead of the Windows `find` command, unless the path to the Windows `find` command is specified on the command line. For example, to ensure that the Windows `find` command is run, use the following syntax: `%WINDIR%\SYSTEM32\FIND`  
As an alternative, you can rename the `find.exe` file in the %SFUDIR%\common directory to `unixfind.exe`.

---

## 4.2 Component summary

SFU consists of a loosely coupled set of components, each individually installed and configured.

<b>Client for NFS</b>	Enables Windows 2000 clients to mount NFS exports as if they were ordinary Windows shares.
<b>Server for NFS</b>	Exports (shares) directories on a Windows 2000 server using NFS.
<b>Gateway for NFS</b>	Shares (relays) NFS exports as Windows shares, allowing any Windows client to access them without installing any NFS client software.
<b>Server for PCNFS</b>	Enables Windows 2000 to act as a PCNFS server, providing seamless user authentication services when connecting to NFS servers.
<b>UNIX utilities</b>	Provides a subset of UNIX commands to be run natively from Windows 2000. See Appendix A, "SFU UNIX utilities" on page 243 for more information.
<b>Korn Shell</b>	Provides an implementation of the Korn shell for running UNIX shell scripts from Windows 2000.
<b>Telnet Client</b>	Enables character-based and script-based remote access and administration.
<b>Telnet Server</b>	Provides security and simplified logins, and supports both stream and console mode.
<b>MMC and WMI</b>	Centralized management of all SFU components from a single application (MMC), as well as from third party software or scripts (WMI).
<b>ActivePerl</b>	Provides an implementation of ActiveState's ActivePerl 5.6, which allows Perl scripts to run natively on Windows 2000.
<b>Server for NIS</b>	Enables a Windows 2000 DC to act as a primary NIS server, integrating NIS domains with Windows 2000 domains.

<b>NIS to AD Migration Wizard</b>	Wizard for migrating NIS information to Windows 2000 Active Directory.
<b>Password Synchronization</b>	Provides 2-way synchronization of passwords, making it easier to implement a consistent password policy for both Windows and UNIX.
<b>User Name Mapping</b>	Associates Windows and UNIX user names, allowing seamless connections to NFS network resources.

---

### 4.3 Installation and customization

SFU is packaged for installation using the Microsoft Installer (MSI) format introduced in Windows 2000. This allows for a flexible and standardized way of installing the application, whether interactively or as an unattended silent installation.

You probably only have one or a few servers to install, so the effort it would take to prepare an unattended installation of the server components would probably be wasted. However, the client installations in your organization could really benefit from a well defined and tested installation script.

The following sections cover the differences between command line and GUI installation to help you choose which one is right for your environment.

#### 4.3.1 Command line installation

When installing an MSI package (in this case, SFU) from the command line, the `msiexec.exe` application is used with a set of parameters. The complete set of available options and parameters is listed in Table 15 on page 131.

A general purpose installation is done using the following syntax:

```
msiexec /i <full path to sfusetup.msi> ADDLOCAL="<component1>
[,<component2>...]" PIDKEY="<key>" SFUDIR="<location>" [/qb|/q]
```

The components to be installed are specified as a case sensitive, comma-separated list parameter to `ADDLOCAL`, and must be enclosed in quotation marks.

Valid component names are:

- NFSServer
- NFSServerAuth

- Pcnfsd
- Mapsvc
- NFSCClient
- NFSGateway
- NIS
- PasswdSync
- Perl
- TelnetClient
- TelnetServer
- UnixUtilities
- CronSvc
- RshSvc

Only the following three components require a reboot to work: Gateway for NFS, Server for NIS, and Password Synchronization.

Table 15. *msiexec.exe* command line options and parameters

Option	Parameters	Explanation
/i	Package ProductCode	Installs or configures a product.
/f	[p o e d c a u m s v] Package ProductCode	Repairs a product. This option ignores any property values entered on the command line. The default argument list for this option is 'pecms.' This option shares the same argument list as the REINSTALLMODE property.  p - Reinstall only if the file is missing o - Reinstall if file is missing or if an older version is installed. e - Reinstall if the file is missing or an equal or older version is installed. d - Reinstall if the file is missing or a different version is installed. c - Reinstall if the file is missing or the stored checksum does not match the calculated value. a - Force all files to be reinstalled. u - Rewrite all required user specific registry entries. m - Rewrite all required machine specific registry entries. s - Overwrite all existing shortcuts. v - Run from source and re-cache the local package.
/a	Package	Administrative installation option. Installs a product on the network.

Option	Parameters	Explanation
/x	Package ProductCode	Uninstalls a product.
/l	[ilwlealrlulclmlolplvl+!] Logfile	Specifies path to log file. The flags indicate which information to log. i - Status messages w - Non-fatal warnings e - All error messages a - Start up of actions r - Action-specific records u - User requests c - Initial UI parameters m - Out-of-memory or fatal exit information o - Out-of-disk-space messages p - Terminal properties v - Verbose output + - Append to existing file ! - Flush each line to the log "*" - Wildcard, log all information except for the v option. To include the v option, specify "!*v".
/p	PatchPackage	Applies a patch. To apply a patch to an installed administrative image, you must combine options as follows: /p <PatchPackage> /a <Package>
/q	n b l r f	Sets user interface level: q, qn - No UI qb - Basic UI qr - Reduced UI with a modal dialog box displayed at the end of the installation. qf - Full UI with a modal dialog box displayed at the end. qn+ - No UI except for a modal dialog box displayed at the end. qb+ - Basic UI with a modal dialog box displayed at the end. The modal box is not displayed if the user cancels the installation. qb- - Basic UI with no modal dialog boxes. Please note that /qb+- is not a supported UI level.

The following example will install the NFS client and the UNIX utilities in the C:\SFU directory without displaying any GUI dialog during the installation:

```
msiexec.exe /i D:\sfusetup.msi ADDLOCAL="NFSClient,UnixUtilities"
PIDKEY="THISISA25CHARLICENSECODE!" SFUDIR="C:\SFU" /qn
```

**Note**

The ADDLOCAL, PIDKEY, and SFUDIR options have to be in upper case!

### 4.3.2 GUI installation

For an interactive GUI installation, insert the CD into your CD-ROM reader and let it autostart or double-click on the sfusetup.msi file in the root of your CD-ROM. It is also possible to start the installation using the setup.exe file, but this mainly checks that your system has the Microsoft Installer service installed on your system and, if not, launches the installation of it.

Because Windows 2000 has MSI support installed by default, there is really no need to go through the MSI verification phase unless you have trouble with your installation.

After starting the installation, you are greeted with the “Windows Services for UNIX Setup Wizard.” After filling out the “Customer Information” dialog box and accepting the license agreement, the installation options dialog shown in Figure 67 appears.

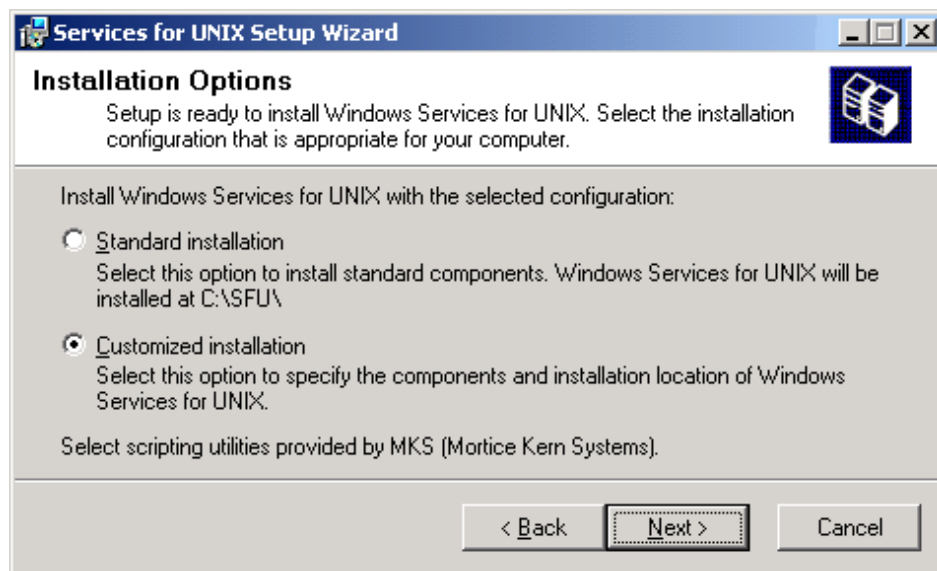


Figure 67. SFU - Installation options

Selecting a standard installation will give you different results depending on your operating system, as outlined in Table 16.

Table 16. Installed components in Standard installation

Component	Professional	Server	Server acting as DC
Telnet Client	X	X	X
Telnet Server	X	X	X
Shell and Utilities	X	X	X
Client for NFS	X	X	X
Server for NFS		X	X
Server for NFS Authentication			X

For full flexibility, we will go through the customized installation, which allows us to select the individual components that we want to install on a particular machine. The Select Components Screen, seen in Figure 68 on page 135, shows all components available for installation on this particular machine. This is the complete set because this is installed on a Windows 2000 Server. A Windows 2000 Professional machine would, for example, not show the NFS Gateway component.



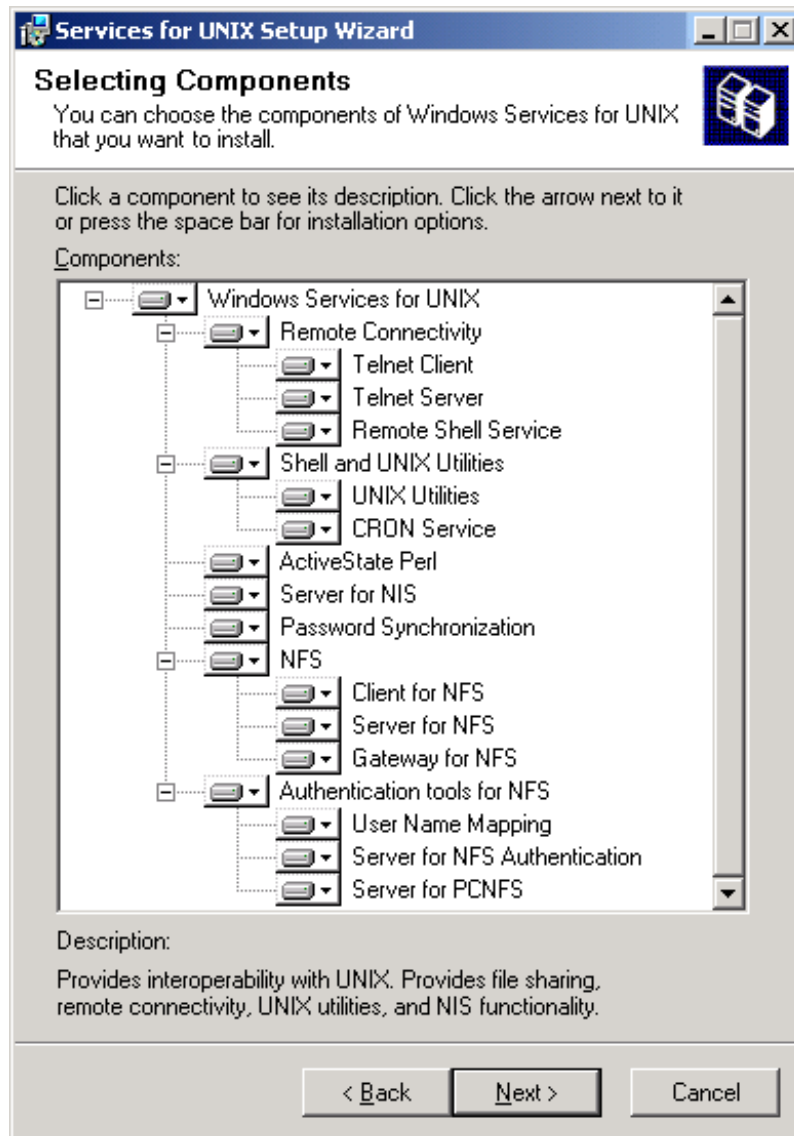


Figure 68. SFU - Selecting components

If a conflicting selection of components is made, such as both Gateway for NFS and Client for NFS, an error message will appear, as shown in Figure 69 on page 136, and you will have to deselect one or both to be able to continue the installation.



Figure 69. SFU - Conflicting components

Please note that if you select the ActiveState Perl component, a separate license agreement will show up. You will have to specifically accept it to continue the installation.

Next, you have to specify the installation location, which defaults to %SystemDrive%\SFU. It is recommended that you accept this location, but if you decide to change it, make sure that the final path does not contain blanks (for example, C:\Program Files\SFU), because this may cause problems with NFS and some UNIX utilities.

If you have installed any of the following components, the machine has to be rebooted before you will be able to start using them:

- Gateway for NFS
- Server for NIS
- Password Synchronization

This concludes the installation. You should now be able to start configuring the various components using either MMC or WMI.

#### 4.3.3 GUI uninstallation and modification

When executing the setup file (sfusetup.msi) again after at least one SFU component has been installed, the SFU Maintenance Wizard is invoked.

From here, you have three options, as shown in Figure 70 on page 137.



Figure 70. SFU - Maintenance Wizard

**Repair or reinstall** This option does not allow you to change any options for installed components, but if you accidentally deleted a file or removed any shortcuts, you can restore the missing files.

**Add or remove** For adding or removing specific components.

**Remove All** Completely removes SFU from your machine and attempts to restore replaced files (for example, telnet.exe, which gets updated when installing SFU).

---

## 4.4 User and Security components

An integral part of SFU is the user management components that tie together most of the other components by making sure that your credentials are mapped and synchronized correctly.

### 4.4.1 User name mapping server

For accessing resources in your AIX 5L environment from Windows without having to provide username and password all the time, you have to utilize an intermediate service for translation between Windows accounts and UNIX accounts. This service is called User Name Mapping Server, and is installed

on one of your DCs as a bridge between the UNIX NIS database and the Windows 2000 Active Directory.

Starting the Windows Services for UNIX Administration Tool invokes the Microsoft Management Console (MMC) with the sfumgmt.msc snap-in.

Selecting User Name Mapping from the tree pane to the left gives you the panel seen in Figure 71.

User Name Mapping on win2ksrv

Configuration Maps Map Maintenance

User Name Mapping creates an association, or map, between Windows user and group names and UNIX user and group names. To configure User Name Mapping settings, select the type of server used to access UNIX user and group names.

Network Information Service (NIS)

Personal Computer Network File System (PCNFS)

To add simple and advanced maps, use the maps tab.

Refresh interval to synchronize user and group names with User Name Mapping:

Hours:  Minutes:

Figure 71. SFU - User Name Mapping

You can either select NIS as your UNIX user and group database, or simply export the user and group files from your UNIX server and open them as flat files from the User Name Mapping Server using PCNFS. Because NIS gives you a vastly more flexible solution, this chapter will focus on the NIS method. Installing and configuring NIS on your AIX system will not be covered in this book; we assume that you have a fully functional NIS system up and running.

**Note**

Do not use both NIS and PCNFS at the same time to map accounts. If you want to add advanced maps using NIS, first remove maps that were created using PCNFS. Similarly, if you want to add advanced maps using PCNFS, first remove advanced maps created using NIS.

Accepting the default refresh interval of 24 hours and making sure that the NIS radio button is selected (default), we continue by choose the Maps button. The panel shown in Figure 72 on page 139 appears.

User Name Mapping on win2ksrv Reload Apply ?

**Configuration** **Maps** **Map Maintenance**

You can create both simple and advanced maps. When the Windows and UNIX names are identical, select Simple maps. To map one name to several other names or when the names are not identical, use Advanced maps.

**Simple maps**

Select the name of the Windows domain that contains the Windows user or group names that you want to map.

Windows domain name:

Enter the NIS domain and NIS server name (optional) that contains the user or group names you want to map.

NIS domain name:

NIS server name (optional):

To create maps, click Apply. User Name Mapping creates the maps automatically.

**Advanced maps**

To map user names, click Show User Maps. To map group names, click Show Group Maps.

[Show User Maps](#) [Show Group Maps](#)

Figure 72. SFU - Simple user mapping

In an ideal environment, all user and group names would be identical on both platforms, and we would be fine with the simple maps configuration. In reality, it is hard to imagine that this ever could be the case, because there is a fundamental difference in the administrative accounts being root in AIX and administrator in Windows 2000.

Figure 73 on page 140 shows the advanced user maps where we simply select the Windows 2000 domain we want to work with, in this case, the local user database on WIN2KSRV and our NIS domain, which we have called nisdomain.com. The NIS server name is optional, but we have entered win2kpvt for reference.

By clicking the List Windows Users and List UNIX Users buttons respectively, the list boxes are populated with the current accounts from each database.

Windows domain name:  NIS Domain name:

NIS server name (optional):

Windows users:

UNIX users:

Unix Users	UID
<unmapped>	-2
ahlen	202
test1	201

Windows user name:  UNIX user name:

To create a map, enter user names you want to map, and click Add.

Mapped users:

Windows User	UNIX Domain	UNIX User	Uid
\\WIN2KSRV\ahlen	nisdomain.com	ahlen	202
\\WIN2KSRV\Ullis	nisdomain.com	test1	201

Display simple maps in Mapped users list

Figure 73. SFU - Advanced user mapping

By selecting one entry from each list of users and clicking **Add**, the **Mapped users** list at the bottom of the panel will be updated with your selection.

It is perfectly OK to map several Windows accounts to one AIX account, which could come in handy if you have multiple administrative accounts in Windows that all should be equivalent to root in AIX.

Similarly, Windows 2000 security groups can be mapped to AIX groups, as shown in Figure 74 on page 141.

Windows domain name:

NIS Domain name:

NIS server name (optional):

Windows groups:

Windows Groups
PasswordPropDeny
Power Users
Replicator
<b>Residents</b>
TelnetClients

UNIX groups:

Unix Groups	GID
sys	3
system	0
usr	100
uucp	5
<b>visitors</b>	<b>202</b>

Windows group name:

UNIX group name:

To create a map, enter group names you want to map, and click Add.

Mapped groups:

Windows Group	UNIX Domain	UNIX Group	Gid
\\WIN2KSRV\Residents	nisdomain.com	visitors	202

Display simple maps in Mapped groups list

Figure 74. SFU - Group mapping

After mapping your users and groups between the two environments, do not forget to click **Apply** in the upper right corner before you quit.

With all user and group mapping up and running, you are ready to explore the rest of the components in SFU.

#### 4.4.2 Password synchronization

Password synchronization will help you keep your UNIX and Windows 2000 user account passwords synchronized. It is not connected to the User Name Mapping service, and requires the UNIX and Windows 2000 account names to be identical. This is particularly important because Windows 2000 is not case sensitive and you may have created the accounts with the first letter

capitalized (Joe instead of joe) without even thinking about it. If your user accounts are not defined exactly the same, you should consider renaming your Windows 2000 accounts because this would pass unnoticed by your users, whereas changing the UNIX accounts would not. Should the naming conventions used in your two environments be totally different from each other, the situation becomes more tricky and you probably have to re-issue all your user accounts, get another product to do the job for you such as Tivoli SecureWay Global Sign-On, or you would have to drop the whole idea.

If you have your two user databases in sync and the only dissimilarities are the character casing, you could turn off the case sensitivity. However, it would still be possible to create two AIX accounts with different names that would correspond to the same Windows 2000 account and produce unpredictable error messages.

Once you have your user accounts lined up, you can start configuring the product. We suggest you start in the AIX end by copying the <CD-ROM>\unix\bins\ssod.a42 file to your /usr/bin directory and rename it ssod. Make sure that the file permissions are set to 555 (r-xr-xr-x).

Next, copy the <CD-ROM>\unix\bins\sso.cfg to your /etc directory and rename it sso.conf. Make sure that the file permissions are set to 644 (rw-r--r--).

The following screen is a short description of the sso.conf file without all the in-file comments.

```
ENCRYPT_KEY=ASDFhjk11234
PORT_NUMBER=6677
SYNC_USERS=all, -root
SYNC_HOSTS=(win2ksrv.itsc.austin.ibm.com)
USE_SHADOW=1
FILE_PATH=/etc/security/passwd
USE_NIS=0
TEMP_FILE_PATH=/tmp
NIS_UPDATE_PATH=/var/yp/Makefile
CASE_IGNORE_NAME=1
SYNC_RETRIES=1
SYNC_DELAY=15
```

The different options are documented in the sso.conf file itself; the following section details some changes you must make before it will work on your AIX 5L system.

**ENCRYPT\_KEY** This character string is used to decrypt password change messages from Windows computers, and must match the encryption key set in your Windows



2000 server.

Default: ASDFhijkl1234. You should definitely change this. In the Windows 2000 GUI, there is a button that will generate a new random character string for you.

**PORT\_NUMBER** This is the TCP/IP port the ssod daemon listens to for password change messages from the Windows 2000 server.

Default: 6677.

**SYNC\_USERS** A list of users for whom passwords are synchronized. All others are ignored. Make sure you disable root from synchronizing passwords by specifying -root as an option.

Default: all.

**SYNC\_HOSTS** A list of the Windows 2000 servers participating in password synchronization with this AIX machine.

**USE\_SHADOW** Indicates whether the machine is using a shadow passwd file or not.

Default: 1.

**FILE\_PATH** Full file path of the file that will be updated with user's password when password change requests come from a Windows 2000 server.

Default: /etc/shadow. You must change this to /etc/security/passwd for the synchronization to work.

**USE\_NIS** If you use NIS, change this to 1 to properly propagate password changes to the NIS database.

Default: 0.

**TEMP\_FILE\_PATH** Specifies a path name where temporary files can be created if this should become necessary. We recommend that you change this to /tmp.

Default:.

- NIS\_UPDATE\_PATH** In case NIS is used, this file is executed to update the NIS database.  
Default: /var/yp/Makefile.
- CASE\_IGNORE\_NAME** Defines whether the comparing of AIX and Windows 2000 user names should be case sensitive or not.  
Default: 1.
- SYNC\_RETRIES** Number of times the ssod daemon will try to synchronize passwords with Windows 2000 servers.  
Default: 1.
- SYNC\_DELAY** Delay between sync retries, in seconds.  
Default: 15.

Start the ssod daemon with the -v (verbose) parameter to verify that all configuration information is correct. To make sure that ssod daemon starts on every reboot, add the following entry at the end of the /etc/inittab file:

```
ssod:23456789:respawn:/usr/bin/ssod >/dev/null 2>&1
```

This concludes the AIX side of the configuration; we will now go through the Windows 2000 part.

**Note**

If you have password restrictions in place in either environment, you could run into trouble when trying to synchronize the passwords. Make sure that the passwords restrictions, if any, are consistent.

We start off with the MMC snap in for SFU, and select the **Password Synchronization Service** from the tree on the left-hand side. The first panel, shown in Figure 75 on page 145, is the default setup, containing the basic configuration parameters from the AIX /etc/sso.conf file, such as ENCRYPT\_KEY, PORT\_NUMBER, and so on. If you have decided to keep the default settings you can leave these parameters at their default values. Here you can also see the previously mentioned **New Key** button that will randomly generate a new encryption key for you that can easily be inserted (copy and paste) into your /etc/sso.conf file.

Password Synchronization on win2ksrv Reload Apply ?

**Default** **Advanced**

The following settings are used as the default settings for all computers running UNIX that participate in password synchronization. Change settings for a specific UNIX computer by using the Advanced tab.

**Direction of password synchronization**

Synchronize password changes from computers that run UNIX to computers that run Windows

Password changes on computers that run Windows are automatically synchronized to computers that run UNIX.

**Security configuration**

Password synchronization uses strong encryption. It uses the following key to decrypt password change messages from UNIX computers. This key should match the key in the SYNC\_HOSTS entry for this computer on each UNIX computer that synchronizes passwords with this computer. Click New Key to generate a new key or type a new key.

Encryption / Decryption key:  New Key

**Port configuration**

This is the port on which Password Synchronization listens for password changes. This value should match the one specified in the SYNC\_HOSTS entry for this computer in the /etc/sso.conf file entry of each UNIX computer that synchronizes passwords with this computer.

Port number:

**Password Synchronization Retries**

Number of retries:

Interval between retries:  seconds

**Logging**

Results of synchronization are logged automatically. To log intermediate steps in synchronization attempts, select the check box below.

Enable extensive logging

Figure 75. SFU - Default password synchronization

For this installation, we will leave the Direction of password synchronization checkbox unchecked because SFU does not come with a compiled version of the UNIX-to-Windows synchronization module for AIX. For those of you who need this functionality, the source code for the module is provided on the SFU

CD and there is an updated 3DES encryption source library on the Microsoft Website:

<http://www.microsoft.com/downloads/search.asp>

See Figure 76 for search criteria.

The screenshot shows a search interface for Microsoft downloads. The 'Product Name' dropdown is set to 'Windows Services for UNIX' and the 'Operating System' dropdown is set to 'Unix'. Under 'Sort By', 'Title' is selected. A 'Find It!' button is visible. Below the search criteria, the results are displayed as a table titled 'Downloads sorted by title -- Windows Services for UNIX -- Unix'.

Date	Title	Version	Size/Time (@ 28.8)
22 Jan 2001	<a href="#">Services for UNIX 2.0 (Triple DES Library)</a>	2.0	60 kb / 1min

Figure 76. SFU - Updated 3DES source library on Microsoft download

Moving on to the advanced section, as seen in Figure 77 on page 147, we add the name of our AIX machine to the list of computers that will be synchronized with our Windows 2000 server.

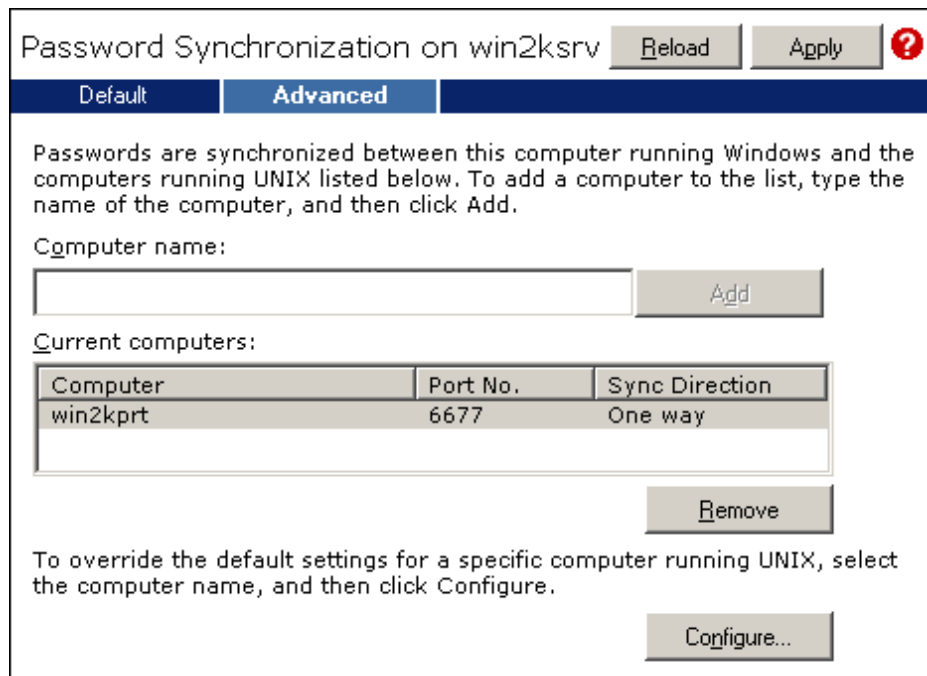


Figure 77. SFU - Advanced password synchronization

Multiple AIX server connections can be customized individually by clicking the **Configure** button. This will bring up the panel shown in Figure 78 on page 148, where you can specify connection unique encryption keys and port numbers.

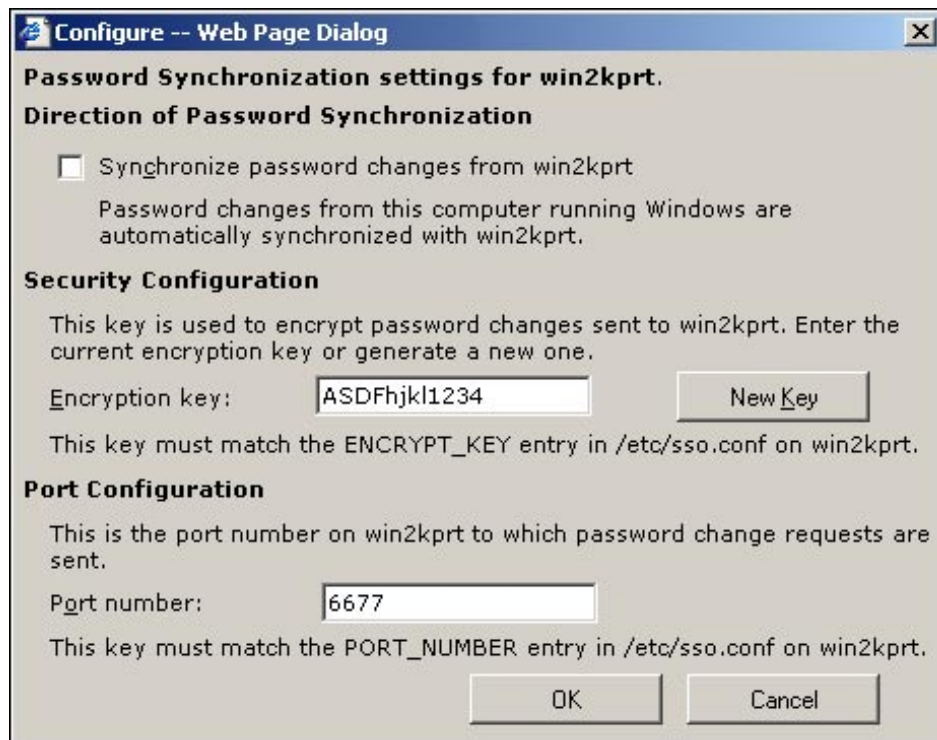


Figure 78. SFU - Advanced individual password synchronization

By default, the PasswordPropDeny group is created in your Windows 2000 domain and is automatically populated with the administrator accounts (that is, all members of the administrator groups). Members of this group are not synchronized with AIX when they change their passwords, so an entry will be added to the Eventlog informing you about the failure of the synchronizing operation.

By manually adding the PasswordPropAllow group, users are required to be members of this group to have their passwords synchronized. As long as you do not add the PasswordPropAllow group, all users who are *not* a member of the PasswordPropDeny group are processed for password synchronization.

#### Security Summary

If PasswordPropAllow does *not* exist, the effect is the same as if it did exist with *all* user names in it.

If PasswordPropDeny does *not* exist, the effect is the same as if it did exist with *no* user names in it.

The PasswordPropAllow and PasswordPropDeny groups in Windows 2000 are used in conjunction with the SYNC\_USERS entry in the /etc/sso.conf file in AIX; if a user's password cannot be synchronized from Windows 2000 to AIX, it cannot be synchronized from AIX to Windows 2000. By default, all AIX users will be synchronized. You should change this behavior to exclude root by adding -root to the SYNC\_USERS parameter.

### 4.4.3 Server for NIS

Server for NIS integrates Network Information Service (NIS) and Windows 2000 Active Directory by allowing a Windows 2000 DC to act as a NIS server for one or more NIS domains. If you have multiple DCs in your domain and one of them is acting as a Master NIS server, the others could be installed as slave servers. It is also possible to mix Windows 2000 and UNIX slave servers in the same NIS domain. Windows 2000 DCs will use AD replication to synchronize NIS changes and yppush to propagate changes to the UNIX-based NIS servers.

By storing the NIS map data in Active Directory, Server for NIS extends the Active Directory schema to accommodate both standard and non-standard NIS maps. Hence, when installing Server for NIS in a domain, you have to be logged in as a member of the Schema Admins group. Remember that changes to the schema are irreversible, so if you install Server for NIS and configure it, even uninstalling the product will not remove the changes in your schema.

The administrator can easily create, modify, and delete user accounts for Windows and UNIX domains at the same time. An example of this is illustrated in Figure 79 on page 150.

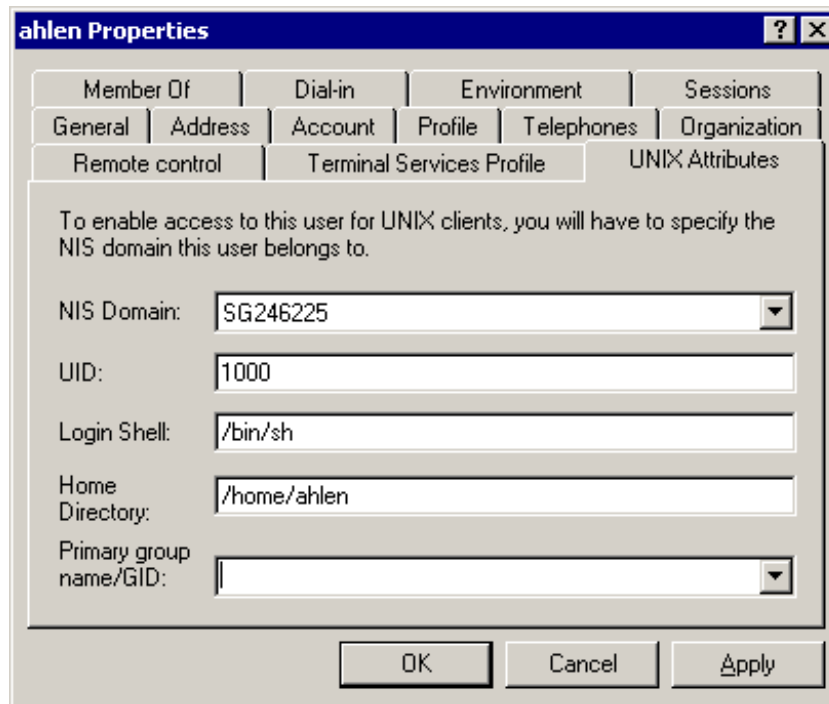


Figure 79. SFU - UNIX properties for users in AD

After installing *Server for NIS*, you need to migrate the current NIS maps from your UNIX-based NIS server, either by using the NIS Server Migration Wizard, or by using the command-line utility. If you have multiple NIS domains, you can migrate all of them to the same Windows 2000 DC and optionally merge them into one new NIS domain.

#### 4.4.4 NIS to AD Migration Wizard

SFU comes with a Migration Wizard that will help you migrate your NIS domains to Active Directory. If you have several NIS domains in your organization, the wizard will help you consolidate these into fewer or even one new NIS domain within Active Directory.

For smaller migrations, there is also a command line utility available called `nis2ad`.



---

## 4.5 File system components

The file system components provided with SFU are all NFS related. NFS is the most common way of sharing Filesystem or directories in the UNIX world. Unfortunately for the Windows community, the NFS protocol is not compatible with Server Message Block (SMB) protocol, which is the way traditional Windows shares are used. A solution to this is to add SMB functionality to AIX 5L or to add NFS functionality to Windows 2000. This chapter will describe the latter, while Chapter 3, “PC connectivity solutions” on page 29 talks about adding SMB functionality to AIX 5L.

### 4.5.1 Client for NFS

Client for NFS is intended for installation on client computers rather than on a server. The only reason you would want to install Client for NFS on a server is when you have an application running on the server that requires access to files available on an NFS export. Remember that you cannot install Client for NFS and Gateway for NFS on the same machine (as seen in Figure 69 on page 136), so you have to decide what level of functionality you need in your environment before installing.

Client for NFS lets you map NFS resources to drive letters on your Windows client computer as if they were ordinary Windows shares, either by using text based commands or by using the Windows 2000 GUI.

#### 4.5.1.1 Text based commands

When mapping drives from scripts or from the command prompt using the traditional `net use` command or the standard UNIX `mount` command, there are a few things to consider.

Whether you choose to use `net use` or `mount` is completely transparent, so you can mix and match between the two as you please. The following four Windows 2000 commands all produce the same result:

```
net use * aixserver:/users
net use * \\aixserver\users
mount aixserver:/users *
mount \\aixserver\users *
```

However, mapping a drive with one command and unmapping it with another could produce unwanted results. Examine the following screen dump in which we map a drive using the `mount` command and then remove it with the `net use` command:

```
C:\>mount win2kprt.itsc.austin.ibm.com:/home/ahlen *
G: is now successfully connected to win2kprt.itsc.austin.ibm.com:/home/ahlen
```

The command completed successfully.

```
C:\>mount
```

Local	Remote	Properties
G:	\\win2kprt.itsc.austin.ibm.com\home\ahl~	UID=-2, GID=-1 rsize=32768, wsize=32768 mount=soft, timeout=0.8 retry=5, locking=yes lang=English

```
C:\>net use g: /d
```

G: was deleted successfully.

```
C:\>mount
```

Local	Remote	Properties
G:	win2kprt.itsc.austin.ibm.com:/home/ahlen	Unavailable

```
C:\>umount g:
```

Disconnecting G: win2kprt.itsc.austin.ibm.com:/home/ahlen  
The command completed successfully.

```
C:\>mount
```

Local	Remote	Properties
-------	--------	------------

As you can see, the `net use g: /d` command successfully removes the mapping, but the resource is still shown as unavailable in the mounted file systems list.

Issuing the `umount` command removes it from the mounted file systems list as well.

### Note

If you export the root directory / on your AIX server, Client for NFS will not be able to mount it using the regular syntax of:

```
net use * \\Servername\ OR net use Servername: /
```

Instead, you have to mount the root directory using an exclamation mark (!) at the end. For example:

```
net use * \\Servername\!
```

The following screen shows the different flags and options available for the `mount` and `umount` commands on AIX 5L and Windows 2000:

AIX 5L mount commands:

```
Usage: mount [-fipr] [-n Node] [-o Options] [-t Type] [-{v|V} Vfs]
        [-a | all | [[Node:]Device] [Directory]]
```

```
Usage: umount [-sf] {-a|-n Node|-t Type|all|allr|Device|File|
        Directory|Filesystem}
```

Windows 2000 SFU mount commands:

```
Usage: mount [-o options] [-u:username] [-p:<password | *>]
        <\\computername\sharename> <devicename | *>
```

```
Usage: umount [-f] <-a | drive_letters | network_mounts>
```

```
-a    Delete all NFS network mount points
-f    Force delete NFS network mount points
```

Evidently there are quite a few differences between the two platforms that do not necessarily introduce any problems unless you rely on mounting file systems from shell scripts that will run on both platforms. The change of syntax is more of an inconvenience for UNIX gurus who know the mount parameters by heart. In this case, using the `net use` command could be easier.

### Note

Using the `mount` command when connecting to an NFS export produces slightly less overhead when establishing the connection than using the `net use` command.

When the connection is in place, there is no difference in performance.

Before mounting an exported filesystem from an AIX host, or if you have problems finding a mount point, you could use the `showmount.exe` command to list the available resources on your host. The options available are:

- a** Show all mount points on host
- d** Show directories mounted on host
- e** Show export list on host

For example, to list all available mount points on `win2kpvt`, type the following command:

```
showmount -a win2kpvt
```

This will produce an output similar to this screen:

```
C:\>showmount -a win2kpvt
All mount points on win2kpvt:
win2ksrv.itsc.austin.ibm.com : /home/ahlen
win2ksrv.itsc.austin.ibm.com : /home/ullis
win2ksrv.itsc.austin.ibm.com : /development/kernel
win2ksrv.itsc.austin.ibm.com : /residents
```

The NFS client does not have a lot of configuration options. The only option you probably want to set or change is the user name mapping server name.

`NFSAdmin.exe` is the tool to use when configuring the client from the command line. It accepts the following options:

```

C:\>nfsadmin client /?

Usage: nfsadmin client [\\computer name] start | stop | config config_options

config_options are
  mapsvr = server      Use specified server for User Name Mapping.
  preferTCP = yes|no   Set TCP as the preferred transport protocol.
                      Uses UDP otherwise.
  mtype = hard|soft    Specify the type of mount.
  retry = number       Set the number of retries for a soft mount.
  timeout = duration   Set the timeout(in seconds) for an RPC call.
  perf = default       Reset performance parameters to default values.
  rsize = size         Set the read buffer size (in KB).
  wsize = size         Set the write buffer size (in KB).
  fileaccess = mode    Specify the permission mode of the file.
                      These are used for new files created on NFS
                      servers. Specified using UNIX style mode bits.

```

For example, to set the map server name to win2ksrv as well as restoring the performance parameters to default values, you would type the following command:

```
nfsadmin client config mapsvr=win2ksrv perf=default
```

To verify your settings, simply type `nfsadmin client` and it will show the current settings:

```

C:\>nfsadmin client

The following are the settings on localhost

Mapping Server      : win2ksrv
Prefer TCP          : No
Mount Type         : SOFT
Retries            : 5
Timeout            : 0.8 seconds
Read Buffer Size   : 32 KiloBytes
Write Buffer Size   : 32 KiloBytes

File Settings
  User             : rwx
  Group            : r-x
  Others           : r-x

```

Using the `perf=default` parameter does not restore the File Settings if they have been changed. Instead, you will have to add the `fileaccess=755` parameter for this change to take place.

#### 4.5.1.2 GUI based commands

NFS mapping from the GUI is nicely integrated into the Windows 2000 networking system, making NFS resources fully browseable, just as you would browse your Windows machines for resources.

As the NFS Client adds itself to your network browser, you can find it when you click **My Network Places** -> **Entire Network**, as shown in Figure 80.

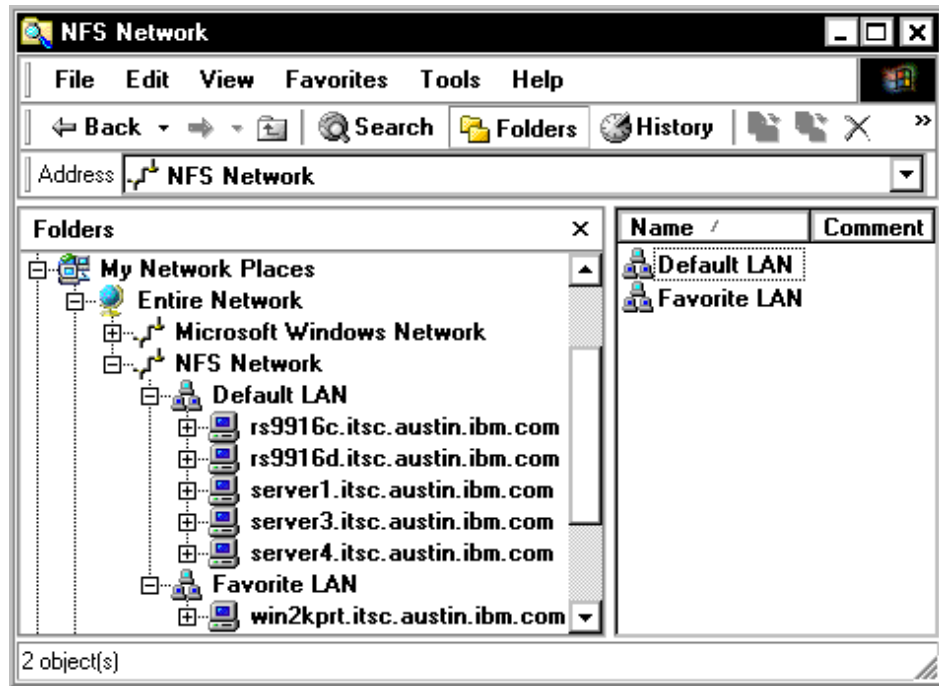


Figure 80. SFU - NFS Network browsing

Notice how the NFS Network is divided into two groups: Default LAN and Favorite LAN. The Default LAN group is a dynamic group populated by a TCP/IP broadcast. The parameters for configuring this is found in the registry under the key HKLM\SYSTEM\CurrentControlSet\Services\Client for NFS\NFS LANs\Default LAN, as shown in Figure 81 on page 157.

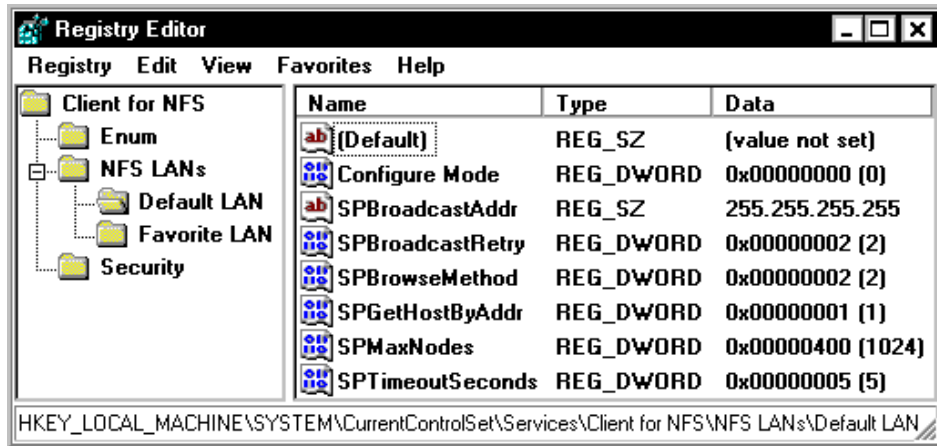


Figure 81. SFU - Default LAN registry values

It is not recommended that you change any of the configuration keys unless you are sure what you are doing, as this could easily lock up your networking subsystem.

Occasionally, the Favorite LAN group disappears from your NFS Network if you have not added any entries to it. If this happens, you will have to add it again manually by editing the registry. An example of this is illustrated in the .reg file on page 158. Being a static group (that is, the content will not change unless you explicitly change it), you have to add NFS hosts by right-clicking on the group and selecting Add/Remove Hosts from the menu. This will bring up the dialog box shown in Figure 82.

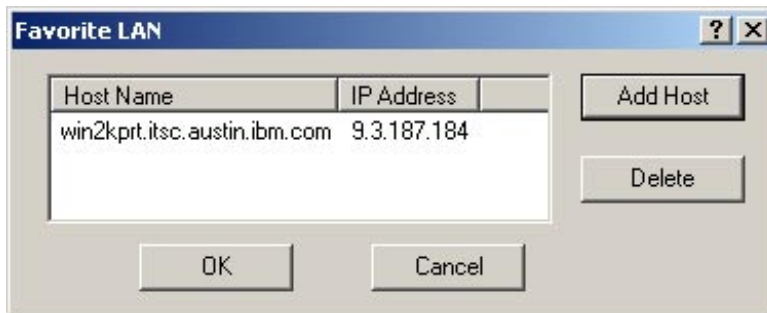


Figure 82. SFU - Add hosts to Favorite LAN

Here you can add or remove hosts simply by selecting **Add Host** or **Delete**. When adding hosts, entering the IP-address will resolve the host name and vice versa, provided that your DNS is correctly configured.

If you are preparing a client roll-out or have a lot of NFS hosts that you want to add to the Favorite LAN group or a customized group of your choice, the easiest way is probably to prepare a registry file that easily could be added to selected clients.

A sample .reg file for adding NFS groups is shown in the following screen.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ /
Client for NFS\NFS LANs\Favorite LAN]
"Configure Mode"=dword:00000001
"win2kpvt.itsc.austin.ibm.com"="9.3.187.184"

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ /
Client for NFS\NFS LANs\Campus LAN]
"Configure Mode"=dword:00000001
"win2kpvt.itsc.austin.ibm.com"="9.3.187.184"
"server4.itsc.austin.ibm.com"="9.3.240.59"
```

Note that the key name lines have been wrapped for readability. This is signified by the “/” symbol at the end of the line.

When applying the previously mentioned .reg file, you should have a result similar to the one shown in Figure 83 on page 159. Note in particular the Campus LAN group that we added and populated with two NFS hosts from different subnets, which never would have shown up in the Default LAN group.



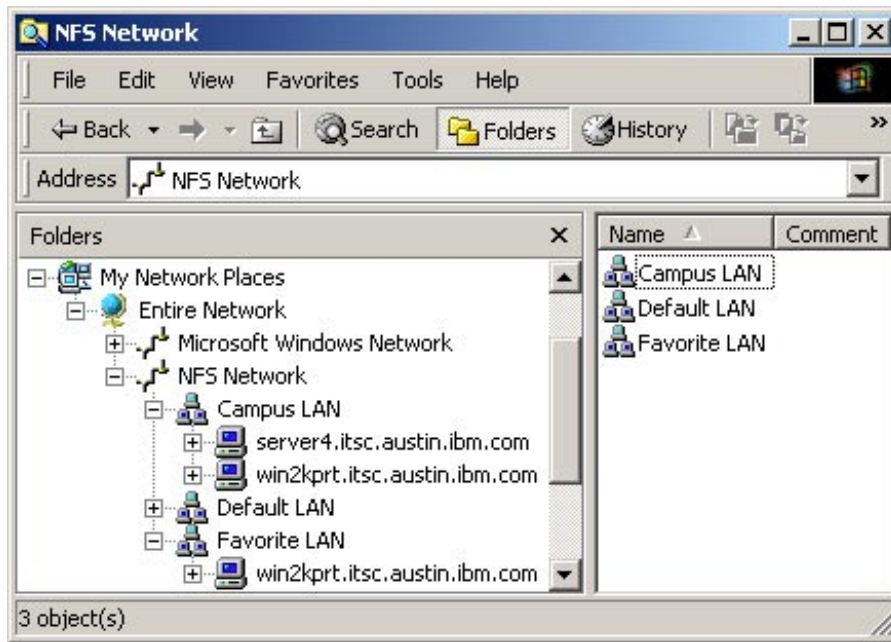


Figure 83. SFU - Custom groups in NFS Network

It is also possible to add a new dynamic, or broadcast based, group by just right-clicking on the **NFS Network** icon and selecting **Add/Remove NFS LANs**. This will bring up the panel shown in Figure 84.

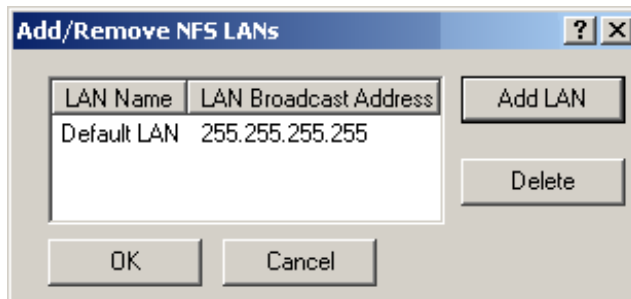


Figure 84. SFU - Add/Remove NFS LANs

By clicking the **Add LAN** button, the panel shown in Figure 85 on page 160 appears. Fill out all the fields.

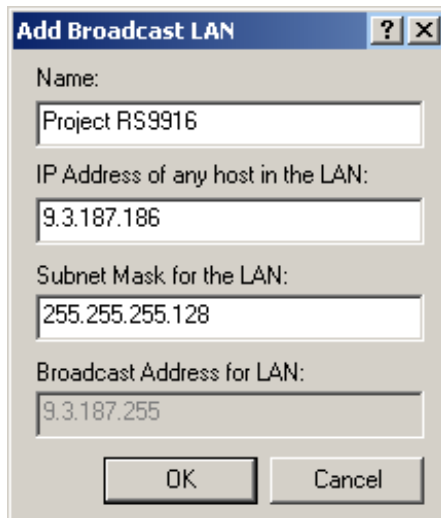


Figure 85. SFU - Add Broadcast LAN

The broadcast address for your LAN will be automatically calculated based on the IP-address and Subnet Mask you provide. The result should be similar to the panel shown in Figure 86.

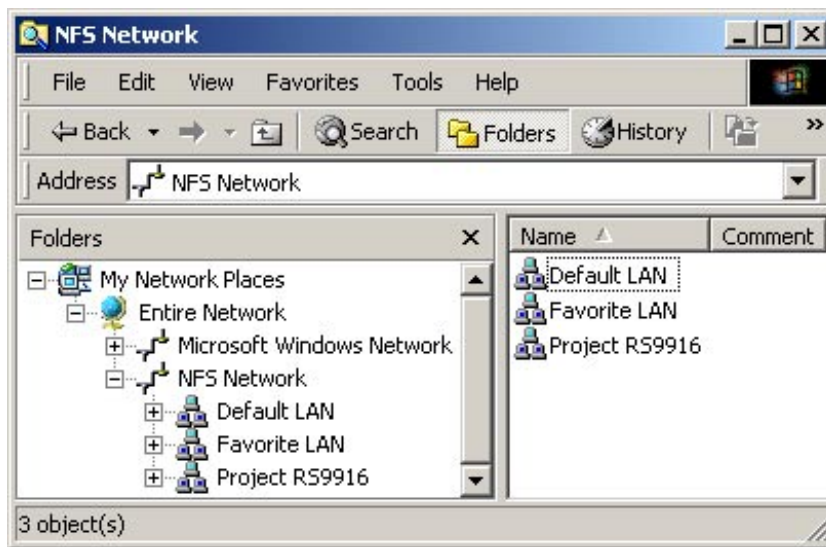


Figure 86. SFU - Added a new dynamic NFS group

To list available resources on a server, either expand it by clicking the plus sign next to it in the browser list, or right-click the server and select

**Properties** from the menu. This gives you a list of exported file systems as well as the access control list for each export. An example of this can be seen in Figure 87.

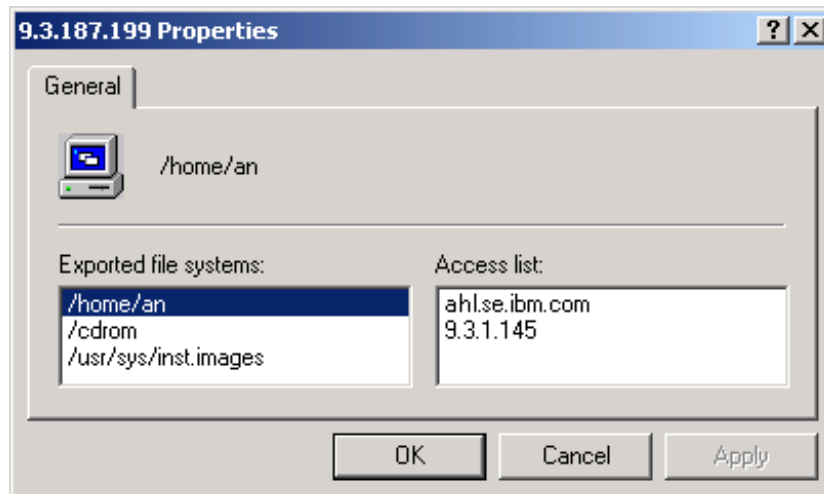


Figure 87. SFU - Server export properties

Configuring the NFS Client from the GUI is as simple as from the command line. Bring up the SFU Administration console (sfumgmt.msc) and select **Client for NFS**, and you will see the Authentication, File Permissions and Performance tabs on the right hand side.

Authentication settings is merely a question of which server you have installed the user name mapping service on. Make sure you have the correct server configured for this, or you will not be authenticated when trying to connect to NFS exports.

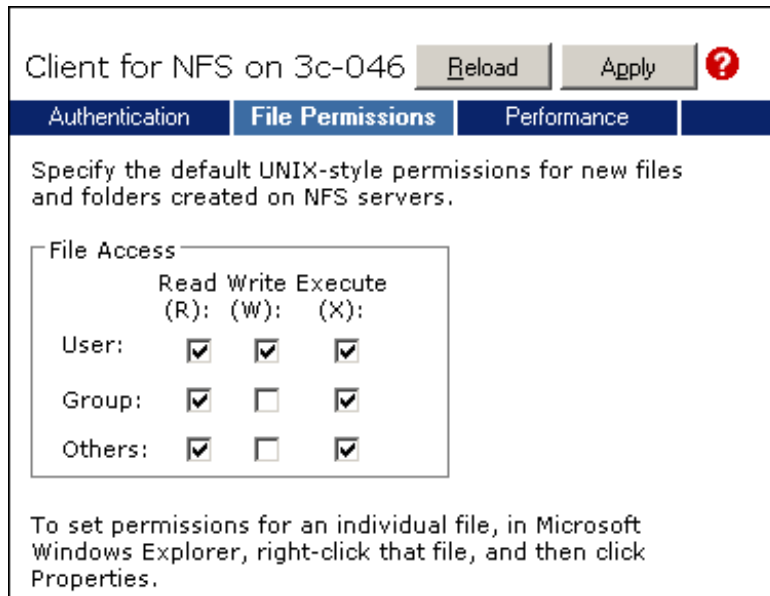


Figure 88. SFU - Client for NFS default file access permissions

The default settings for File Access are shown in Figure 88. This is equivalent to `rwxx-rx-x` or a `UMASK` of `022` in UNIX style.

If you change the settings while you have file systems mounted on your client, the change will not take effect until you remount the file system.

The Performance settings, shown in Figure 89 on page 163, are not really useful unless you have a very homogenous environment where tweaking time-out and buffer sizes could give you some performance improvement.

Client for NFS on 3c-046

Authentication

File Permissions

**Performance**

The following NFS client settings affect NFS server response. Optimal settings depend on your system configuration and network condition

Transport protocol:		UDP ▾
Mount type:		Soft ▾
Maximum number of retries for any operation:		5 ▾
Interval between retries:		0.8 ▾ seconds
Read buffer size:		32 ▾ KB
Write buffer size:		32 ▾ KB

Figure 89. SFU - Client for NFS performance settings

Keep in mind that local Windows 2000 accounts and Windows 2000 domain accounts are two different things. Even though they may have the same name and password, security wise they are considered to be completely different. This can result in hard-to-spot problems with access to files on your NFS exports.

In the following example, we created a local account with the same name and password as the domain account and logged on locally on the client. Mapping a resource from the server works fine, as does reading files, but when we try to create or delete a file, we get an Access Denied message.

The reason for this is that we, unknowingly, only got anonymous access to the NFS export, and therefore only have read rights. A way to spot this is to list your mounted file systems from the command line and look for the UID and GID that you have been authenticated with. This is what the list looked like when we got improper access:

```

C:\>mount

Local      Remote                Properties
-----
G:         \\win2kprt\home\ahlen  UID=-2, GID=-1
                                     rsize=32768, wsize=32768
                                     mount=soft, timeout=0.8
                                     retry=5, locking=yes
                                     lang=English

```

Notice that the UID and GID do not match the user account on the AIX machine. If we instead logout and login again, this time using the domain account, the result is more in line with what we expected to see:

```

C:\>mount

Local      Remote                Properties
-----
G:         \\win2kprt\home\ahlen  UID=202, GID=1
                                     rsize=32768, wsize=32768
                                     mount=soft, timeout=0.8
                                     retry=5, locking=yes
                                     lang=English

```

File access rights are now working the way we anticipated. We can also manually verify, using the user name mapping server console or the AIX passwd file, that UID 202 is in fact the AIX account we mapped to our Windows 2000 account.

#### 4.5.2 Gateway for NFS

Gateway for NFS is a simple way of providing access to NFS exports to clients without having to install any NFS Client code on your Windows 2000 machines. It works, just as the name suggests, as a gateway between SMB shares and NFS exports. The server running the Gateway for NFS component mounts the desired NFS exports and assigns a share name and drive letter for each, as seen in Figure 90 on page 165.

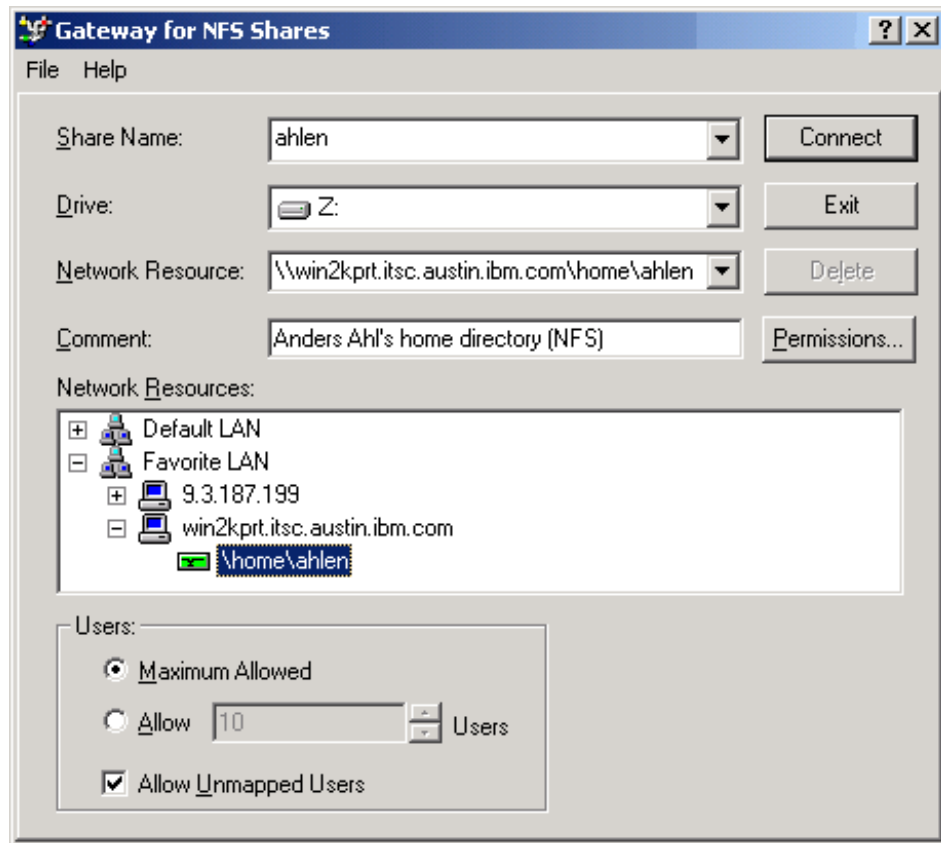


Figure 90. SFU - Gateway for NFS Shares

Clients can then map the SMB share (in this case, ahlen) to their machines just as if it was a share native to the Windows 2000 server. Displaying the Windows 2000 server shares gives a transparent result, as seen in the following screen.

```
C:\>net view \\win2ksrv
Shared resources at \\win2ksrv

Share name  Type    Used as  Comment
-----
ahlen       Disk    Anders Ahl's home directory (NFS)
```

The configuration tool for Gateway for NFS is, for some reason, separated from the MMC and runs as a stand alone application called gwconfig.exe that

you can start by selecting Gateway for NFS Configuration from the SFU menu or find in the %SFUDIR%\common directory.

You will, however, use the MMC to specify the user name mapping server, but after that, all administration is through gwconfig.exe.

After connecting to the “relayed” NFS export from a client using Windows 2000 drive mapping, right-clicking on the drive and selecting **Properties** reveals two unique tabs pertaining to the NFS attributes and options. The first of the two new tabs, NFS Attributes (Figure 91), contains extensive information on permissions, access times, and file attributes.

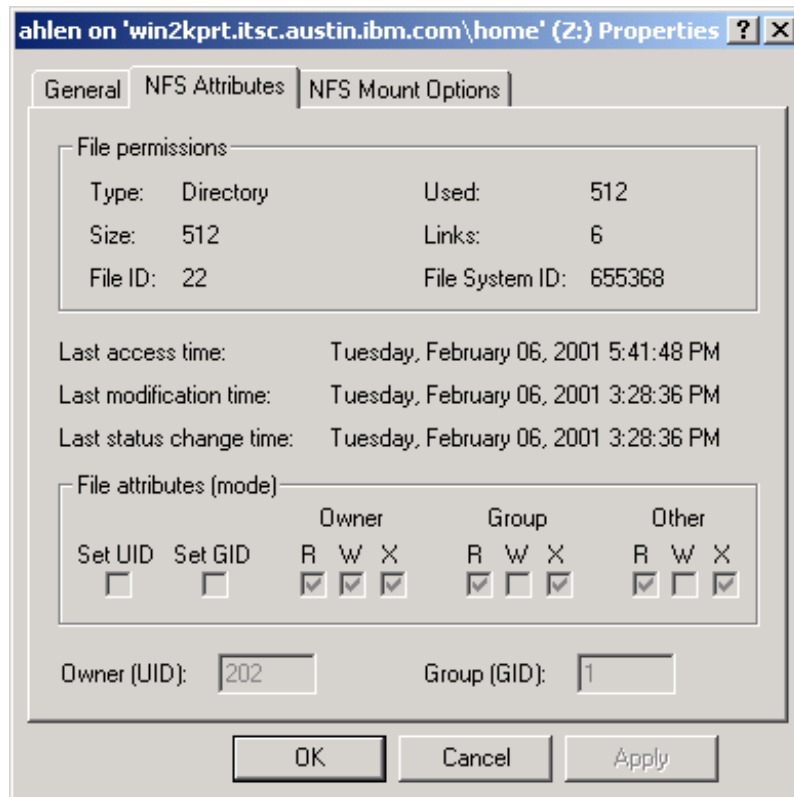


Figure 91. SFU - NFS Attributes tab

The second tab, NFS Mount Options (Figure 92 on page 167), contains mount options as well as the UID and GID with which the authentication to the server was made. For more information about potential problems with Windows 2000 user IDs connecting to NFS exports, see Section 4.5.1.2, “GUI based commands” on page 156.



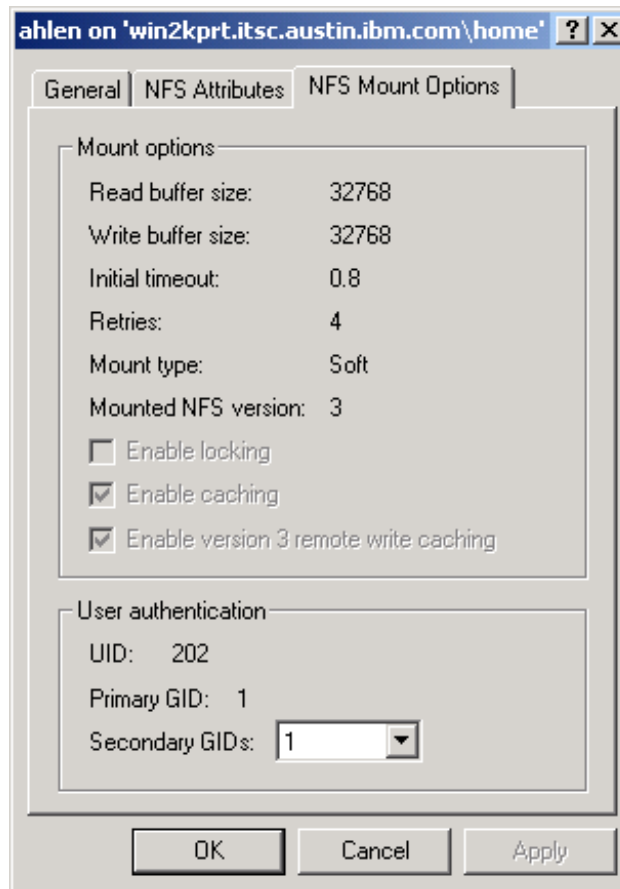


Figure 92. SFU - NFS Mount Options tab

For large networks or environments in which you need the clients to access more than about 20 different NFS exports, Gateway for NFS is not the right choice because it requires a drive letter for each share on the server. Also, because all NFS operations will be funneled through this server, if it is not dedicated to being a file server or an NFS Gateway server, the gateway function will put additional strain on the server as well as on the network (as files are transferred from the AIX server to the gateway server and then to the client, literally doubling the bandwidth requirements of the transaction).

On the other hand, if you have just a handful of NFS exports and do not want to install Client for NFS on all your client machines, Gateway for NFS will definitely make your integration smooth with a zero-footprint client.

### 4.5.3 Server for NFS

Server for NFS allows AIX or Windows 2000 machines to access files on a Windows 2000 server using the NFS protocol. For AIX users, this process is completely transparent, as file level access is determined by the user's UID or GID using the user name mapping server, as well as by local Windows Access Control Lists (ACLs). For maximum security and control, we recommend that the exported file systems on the Windows 2000 server are located on NTFS-formatted file systems, even though this is not a requirement.

Both Version 2 and Version 3 of the NFS protocol are supported, and are implemented using the Open Network Computing Remote Procedure Call (ONC RPC) protocol, as well as the eXternal Data Representation (XDR) protocol between NFS clients and the NFS server.

Establishing an NFS export is very similar to sharing a directory. Right-click on the directory you want to export, select **Properties**, and choose the **NFS Sharing** tab, as shown in Figure 93.

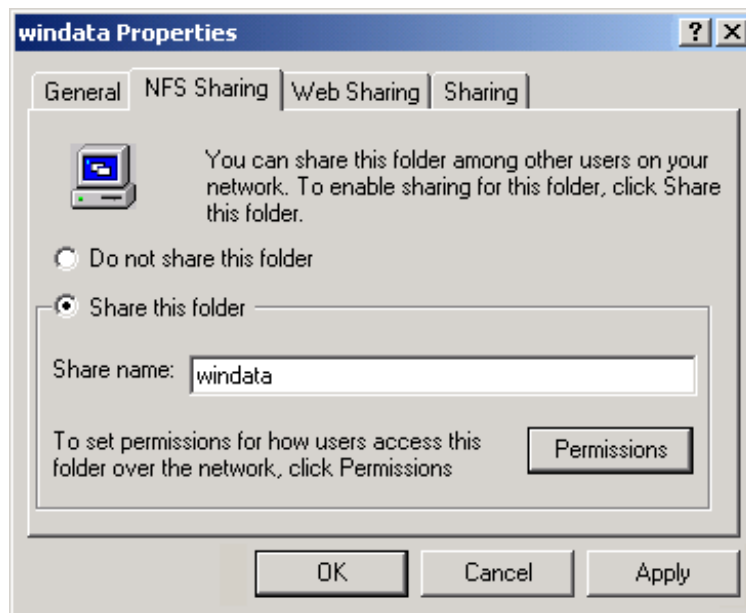


Figure 93. SFU - NFS Sharing tab

The share name defaults to the directory name. If this is acceptable, click **OK** or **Apply**.

Unfortunately the directory does not change its icon (a hand is normally added under the folder) when it is exported, as a traditional Windows share does. To find exported directories (their location, not only their names), you must use the `showmount.exe` command on the command line.

MMC is the tool for configuring the Server for NFS. The user mapping server follows the same procedure as the other tools in SFU.

Logging is new to Server for NFS and enables you to keep track of a set of event types that you specify for logging, as you can see in Figure 94.

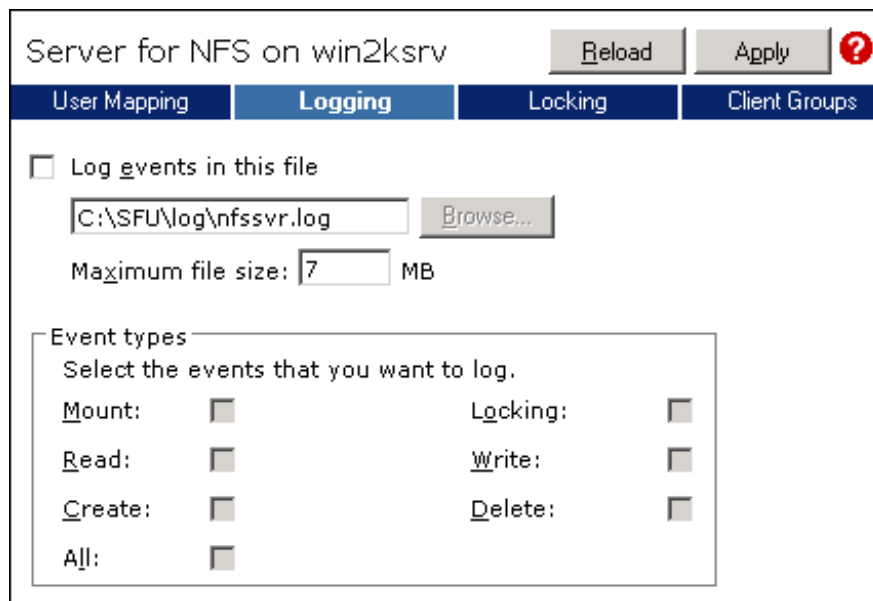


Figure 94. SFU - Server for NFS logging

File locking, as shown in Figure 95 on page 170, is implemented using the Network Lock Manager (NLM) protocol, and allows files accessed through NFS to be locked for exclusive use.

AIX 5L, as with most other UNIX versions, does not enforce lock semantics on files. However, Server for NFS implements mandatory locks, enforced by Windows 2000, even for those locking requests that are received through NFS, ensuring that locks acquired through NFS are visible through the SMB protocol and to applications accessing the files locally.

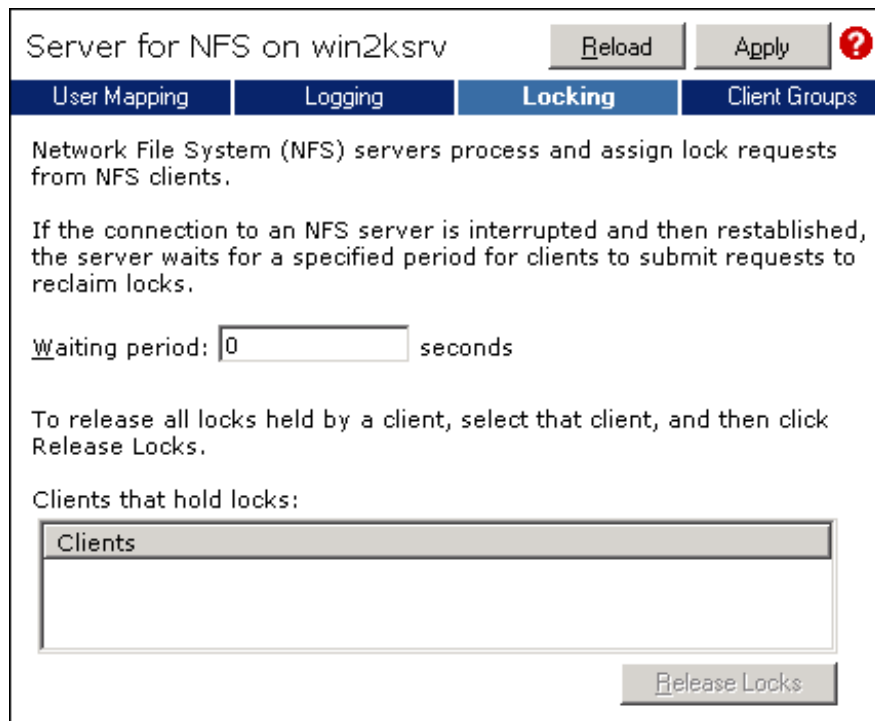


Figure 95. SFU - Server for NFS locking

#### 4.5.4 Server for PCNFS

*Server for PCNFS* provides UNIX authentication information for client computers that cannot use User Name Mapping service, that is, not running a 32-bit Windows system. Because the scope of this book is limited to Windows 2000 clients, the functionality of *Server for PCNFS* will not be discussed.

---

#### 4.6 Telnet components

Remote administration of a Windows 2000 server is best accomplished using the Microsoft Management Console (MMC), which easily configures to your particular needs using snap-ins. It does, however, require that the client you are connecting from be running Windows NT or 2000. Adding Windows 2000 Web administration would get you a bit further, but you would still need a compatible browser on your client system.

Virtually all TCP/IP enabled devices, regardless of operating system, come with a telnet client, so adding a telnet server to your Windows 2000 server could prove very useful.

#### 4.6.1 Telnet server

The Telnet Server included in SFU provides ASCII terminal sessions to Telnet clients using either ANSI, VT-100, VT-52, or VTNT as terminal emulation.

##### 4.6.1.1 GUI configuration

Administration and configuration of the Telnet server is done through the SFU MMC snap-in.

The first set of configuration options are related to authentication. There are two supported methods for authentication: NTLM and plaintext (see Figure 96 for details).

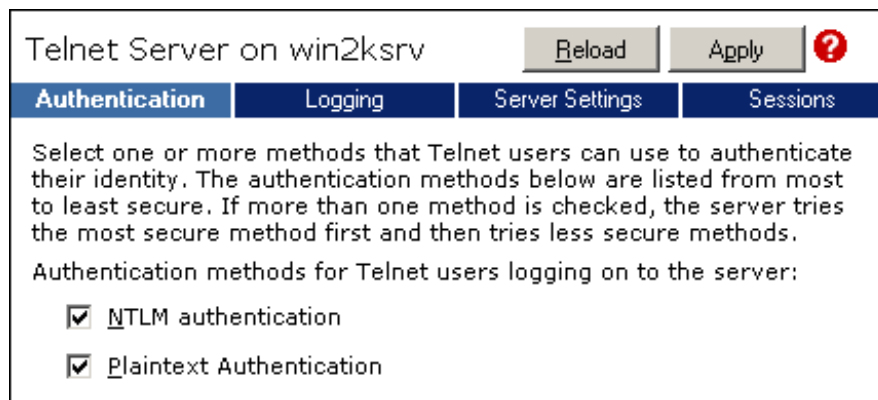


Figure 96. SFU - Telnet Server Authentication options

NTLM encrypts the authentication dialog between the client and the server, but it is a proprietary protocol, and requires that the client is running Windows.

If both methods are selected (default), NTLM will be used first; if it fails, plaintext authentication will take place.

Telnet Sever event logging is, by default, set up to use the Windows 2000 Event Log, generating events for administrators logging on and off, as seen in Figure 97 on page 172.

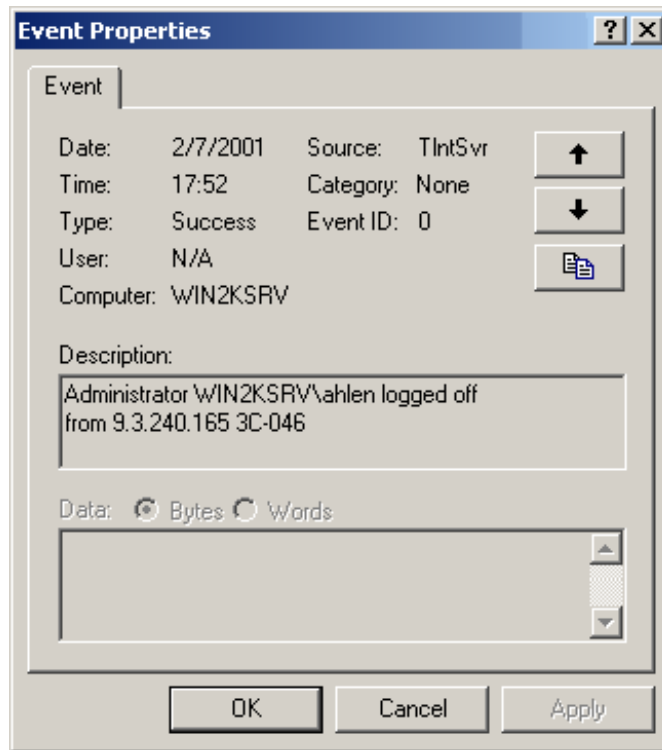


Figure 97. SFU - Telnet Server Event log entry

Logging can be done by specific file. Authentication failures and non-administrators' logon and logoff can also be selected for logging, as seen in Figure 98 on page 173.

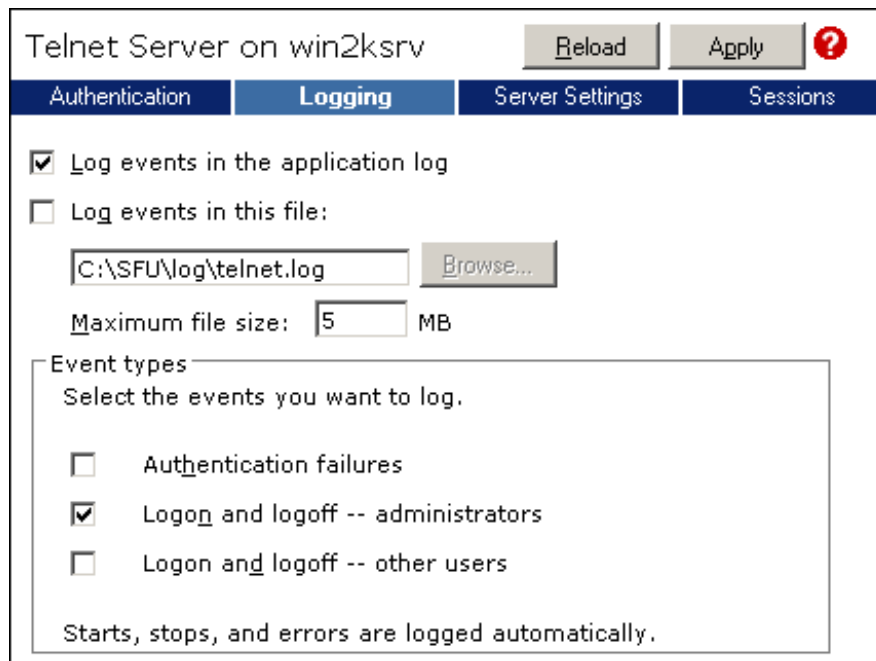


Figure 98. SFU - Telnet Server Logging options

The Server Settings shown in Figure 99 on page 174 are probably nothing you need to worry about except for the Default Domain Name. Make sure that this is set to your Windows 2000 domain name to speed up the login process for users.

Telnet Server on win2ksrv

Authentication
Logging
Server Settings
Sessions

Maximum number of simultaneous connections:

Maximum number of failed logon attempts:

Telnet port:

Mode of operation:

Default domain name:

Disconnect idle client sessions after:  Hours  Minutes  Seconds

Interpret CTRL+A as ALT

Server action after the user ends the Telnet session:

Stop all programs

Continue to run all programs started with the background job (bgjob) command

Figure 99. SFU - Telnet Server Settings

The Maximum number of simultaneous connections defaults to the number of licensed connections you have on your server, and cannot be set higher. Trying to connect to the server when the maximum number of connections has been reached results in the following error message:

Denying new connections due to the limit on number of connections.

To change the maximum number of connections, use Services For Unix administration.

Connection to host lost.

For a slight increase in security (at least for basic port scanners), you could move the telnet port to something above 1024, as long as that does not conflict with other applications on your server.

Finally, the sessions tab shown in Figure 100 on page 175 will let you keep track of the currently active sessions on your server. Also, you have the option of terminating or sending a message to one or several sessions.



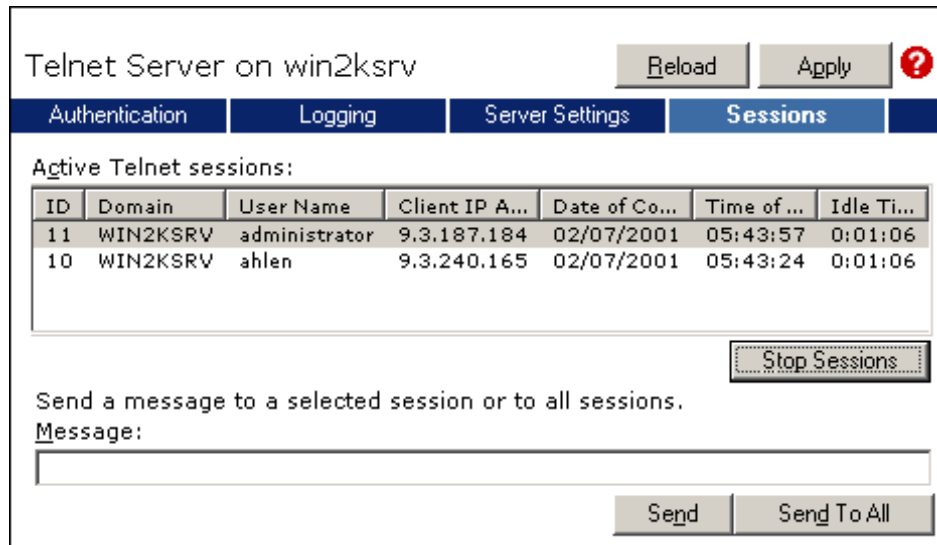


Figure 100. SFU - Telnet Server Sessions

#### 4.6.1.2 Command line configuration

For convenience, the Telnet Server can be administered from the command line using the `tnadmin.exe` tool. Typing `tnadmin.exe` without any options presents the current status of the Telnet Server, as seen in the next screen.

```

C:\>tnadmin

The following are the settings on \\win2ksrv

Alt Key Mapped to CtrlA      : YES
Idle session timeout         : 1 hrs
Max connections               : 5
Telnet port                   : 23
Max failed login attempts    : 3
End tasks on disconnect      : NO
Mode of Operation            : Console
Audit logs                    : +eventvwr
Authentication Mechanism     : NTLM, Password
Default Domain                : win2ksrv
Auditing                      : Login(admin)

State                          : Running
  
```

`tnadmin.exe` comes with an impressive set of options, and even though it is slightly more awkward than using the GUI, there is nothing you cannot do with `tnadmin.exe` compared to the MMC GUI snap-in. The following screen shows you the complete set of options available.

```

C:\>tnadmin /?

Usage: tnadmin [\\computer name] start | stop | pause | continue | -s | -k | -m
| config config_options

-s sessionid      List information about the session.
                  Use "all" for all sessions.
-k sessionid      Terminate a session.
-m sessionid      Send message to a session.
config            Configure telnet server parameters.

config_options are:
  dom = domain      Set the default domain for an unqualified
                  user name.
  ctrlakeymap = yes|no  Set the mapping of the ALT key
  timeout = hh:mm:ss  Set the Idle Session Timeout
  timeoutactive = yes|no  Enable idle session timeout.
  maxfail = attempts  Set the maximum number of login failure attempts
                  before disconnecting.
  maxconn = connections  Set the maximum number of connections.
  port = number      Set the telnet port.
  killall = yes|no    Enable terminating applications started via
                  telnet while disconnecting that session.
  sec = [+/-]NTLM [+/-]passwd
                  Set the authentication mechanism
  fname = file       Specify the name of the audit file.
  fsize = size       Specify the maximum size (in MB) of the audit file.
  mode = console|stream  Specify the mode of operation.
  auditlocation = eventlog|file|both
                  Specify the location for where to log
  audit = [+/-]user [+/-]fail [+/-]admin
                  Specify events to audit

```

## 4.6.2 Telnet client

Windows 2000 comes with a simple Telnet client as part of the installed TCP/IP tools. A major difference between earlier Windows Telnet clients and the Windows 2000 version is that it no longer is a GUI application. For better or for worse, the Windows 2000 Telnet client is now a command line application similar to a traditional AIX Telnet client.

In SFU, the Telnet client is further augmented to support different terminal types, logging functions, and user credentials.

The default Windows 2000 Telnet client will only take two arguments as options: host and port. These arguments are shown in the following screen.

```

C:\>telnet /?

telnet [host [port]]

host      specifies the hostname or IP address of the remote
          computer to connect to.

port      Specifies the port number or
          service name.

```

Compared to previous Windows versions, this is a step back in functionality, despite the change from a GUI application to a command line application, because the old version had support for VT-52, VT-100, and ANSI, as well as a logging function. However, the SFU Telnet client more than compensates for this loss by supporting the features shown in the next screen.

```

C:\>telnet /?

telnet [-a][-e escape char][-f log file][-l user][-t term][host [port]]
-a      Attempt automatic logon. Same as -l option except uses
        the currently logged on user's name.
-e      Escape character to enter telnet client prompt.
-f      File name for client side logging
-l      Specifies the user name to log in with on the remote system.
        Requires that the remote system support the TELNET ENVIRON option.
-t      Specifies terminal type.
        Supported term types are vt100, vt52, ansi and vtnt only.
host    Specifies the hostname or IP address of the remote computer
        to connect to.
port    Specifies a port number or service name.

```

Using the SFU Telnet client when connecting to a Windows 2000 server running the Telnet Server is described in Section 4.6.1, "Telnet server" on page 171. The client will try to authenticate you using the credentials with which you are current logged on to your machine. It is also possible to use the Telnet client interactively by just typing `telnet` without any options. This brings up the Telnet prompt, from which you have a set of options to choose from, as seen in the following screen.

```

Microsoft (R) Windows 2000 (TM) Version 5.00 (Build 2195)
Welcome to Microsoft Telnet Client
Telnet Client Build 5.2000.0328.1

Escape Character is 'CTRL+]'

Microsoft Telnet> ?

Commands may be abbreviated. Supported commands are:

c - close          close current connection
d - display        display operating parameters
o - open hostname [port] connect to hostname (default port 23).
q - quit          exit telnet
set - set          set options (type 'set ?' for a list)
sen - send        send strings to server
st - status       print status information
u - unset        unset options (type 'unset ?' for a list)
?/h - help       print help information
Microsoft Telnet>

```

The Telnet client is great for quick remote administration of both your AIX and Windows 2000 environments. It even supports the use of function keys in AIX `smitty`, which the standard telnet client does not.

---

## 4.7 Shells and utilities

To further facilitate the integration between AIX and Windows 2000, SFU provides a set of common UNIX utilities and a port of the Korn shell. This is very fortunate for AIX environments, because the Korn shell is the default AIX shell, and scripts will most likely to be written for it.

### 4.7.1 Korn shell

The Korn shell can be used either interactively (by specifying `sh.exe` instead of `cmd.exe` when you open a command prompt) or as a script processor (by passing your shell script as an argument to the `sh.exe` file).

### 4.7.2 UNIX utilities

A complete list of the provided UNIX utilities can be found in Appendix A, “SFU UNIX utilities” on page 243.

### 4.7.3 ActiveState ActivePerl 5.6

Perl is an interpreted high-level programming language developed by Larry Wall. As Perl is widely available on most major platforms, Perl has more or less become the preferred scripting language of the Web, as most CGI scripts

are written in Perl. However, Perl is also widely used as a rapid prototyping language and is popular with system administrators who use it for automating day to day tasks. Because Perl is an interpreted language, Perl programs are highly portable across systems.

The port of Perl itself, which is provided with SFU, is done by ActiveState (<http://www.ActiveState.com/>), and even though it can be installed along with the other SFU components, it has its own help file hidden away in the %SFUDIR%\Perl\htmlhelp directory as ActivePerlHelp.chm. It would be a good idea to make a shortcut to this file on your **Start** menu next to the SFU help file.

For the latest version of the documentation, visit:

<http://www.ActiveState.com/ActivePerl/docs/faq/ActivePerlfaq.html>

At the time of writing, the latest version is Build 623 from December 12, 2000, and the version on the CD is Build 613 from March 23, 2000.

---

## 4.8 System administration

No matter how well your system runs, there is always the need to add, remove and change components. The GUI system administration tool of choice for Windows 2000 is the Microsoft Management Console, and for command line administration, the Windows Management Instrumentation lets you write scripts using Windows Scripting Host (WSH).

### 4.8.1 Microsoft Management Console (MMC)

You can use Microsoft Management Console (MMC) to create administrative tools (called MMC consoles) that manage the various components of your Windows system.

MMC does not perform the administrative functions itself, but acts as a common interface to the tools that do. The type of tools you can add to a console must be written according to the MMC specifications, and are called snap-ins.

The MMC in Figure 101 on page 180, taken from the MSDN library (<http://msdn.microsoft.com/library/default.asp>), clearly shows the different parts of the MMC and their respective names.

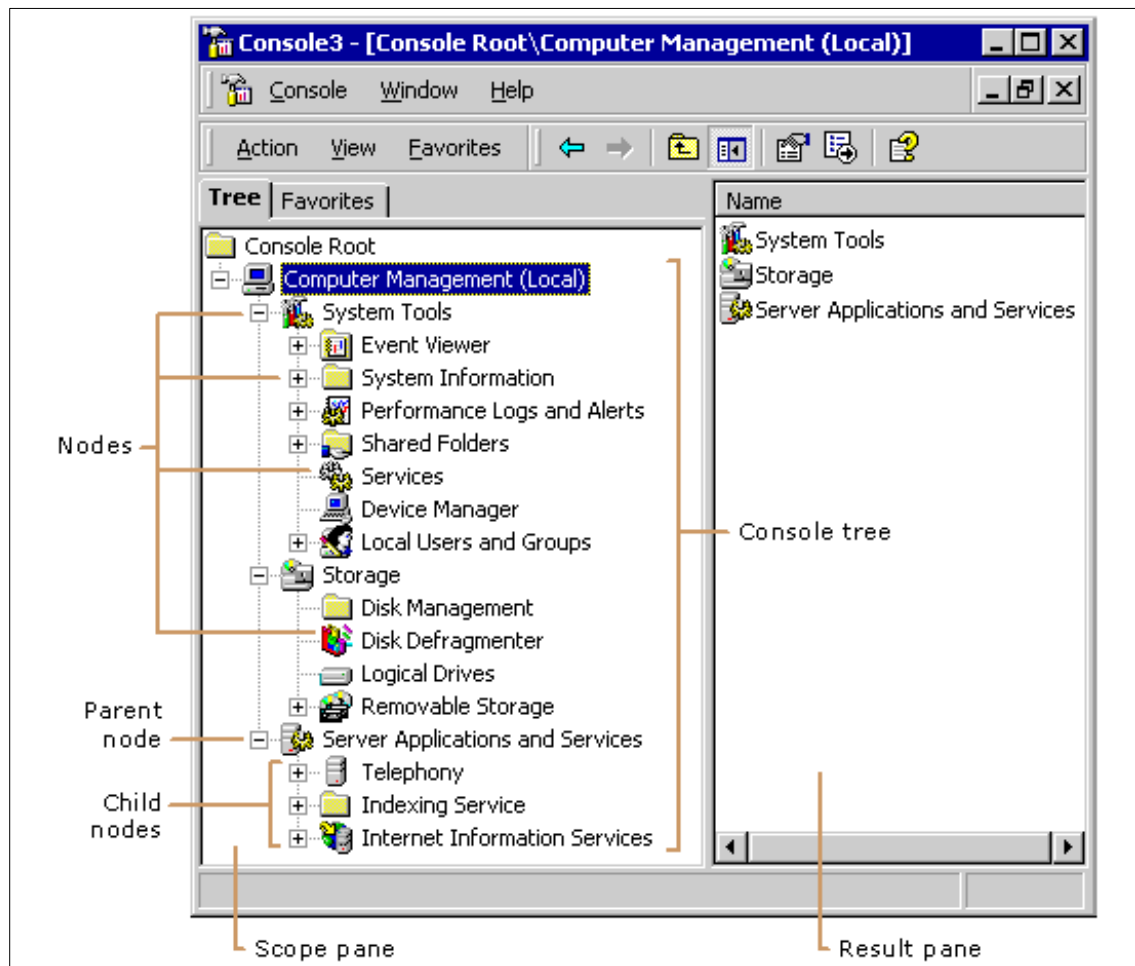


Figure 101. MMC user interface elements

SFU is managed with an MMC snap-in called sfumgmt.msc, which can either be run as a stand-alone or incorporated into any of your present consoles.

You could easily use one console for all your SFU servers and clients, as shown in Figure 102 on page 181.

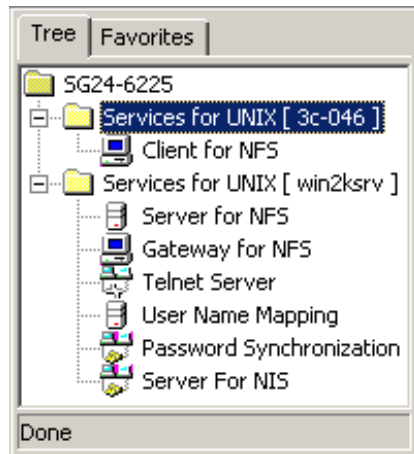


Figure 102. SFU - Servers and clients console

The usage of MMC for administering Windows 2000 components is a big step forward compared to the diverse set of utilities needed in prior versions of Windows. An application providing a management snap-in for MMC is more likely to be adopted into a production environment than one with a 'home-made' administration interface.

---

## 4.9 Windows Management Instrumentation (WMI)

Windows Management Instrumentation (WMI) is Microsoft's implementation of the Distributed Management Task Force's (DMTF) Common Information Model (CIM). CIM is an industry standard schema for instrumentation and management, so WMI can be said to be "CIM for Windows." It covers everything from devices and system processes to application.

For more information about WMI, see:

<http://www.microsoft.com/hwdev/WMI/>





---

## Chapter 5. Terminal emulation solutions

In this chapter, we will discuss solutions for Windows 2000 that provide emulation of AIX 5L terminal services. We will cover utilizing the Common Desktop Environment (CDE), X Window, and how to more efficiently manage your solutions for interoperability by using Windows and AIX graphical applications simultaneously on the Windows 2000 desktop.

---

### 5.1 X Window Display Manager (XDM)

The X Window Display Manager is supported on AIX through the process `dtlogin`. To see if `dtlogin` is running on your AIX 5L system, enter the command `ps -eaf | grep dtlogin`. The `dtlogin` process manages all client XDM requests, and allows for the export of the Common Desktop Environment X Window.

The X Display Manager Control Protocol (XDMCP) is also supported in AIX 5L, and is the mechanism used for an XDM service like `dtlogin` in AIX to export the X Window display over a TCP/IP network. XDMCP works at an application layer level over TCP/IP, like FTP, and is the means by which the client and server work together to properly facilitate the use of X Window on client systems.

In the following sections, we will present three applications, Hummingbird Exceed, NCD's PC-Xware, and WRQ's Reflection, that allow a Windows 2000 environment to make requests to `dtlogin` to export an X Window display and X Window applications. These applications use the XDMCP to make requests of XDM.

---

### 5.2 Hummingbird Exceed

Exceed is a product from Hummingbird Limited that allows you to use graphical applications and utilize the CDE from AIX 5L on a Windows 2000 desktop.

The pre-requisites for this section are that you have both a functional Windows 2000 system and a functional pSeries system running AIX 5L, and that both systems can communicate normally over a TCP/IP network. In this section, we shall be discussing the installation, configuration, and functionality of a trial version of their Exceed Version 7 for Windows 2000 software which is available at:

<http://www2.hcl.com/html/forms/nc/exceed/request.html>

On that page, fill out the short questionnaire and click on **Submit**, then click on the appropriate download icon and specify a path to download Exceed\_Intel\_ver7.exe. Free Technical Support is available during the evaluation period.

### 5.2.1 Exceed installation

Once the download is completed, execute Exceed\_Intel\_ver7.exe. Specify a path to install the Exceed program files into or keep the default path, and click on **Next**.

Now you will be prompted with the title panel for the Exceed installation wizard. Click **Next** and then you will be prompted with the panel shown in Figure 103.

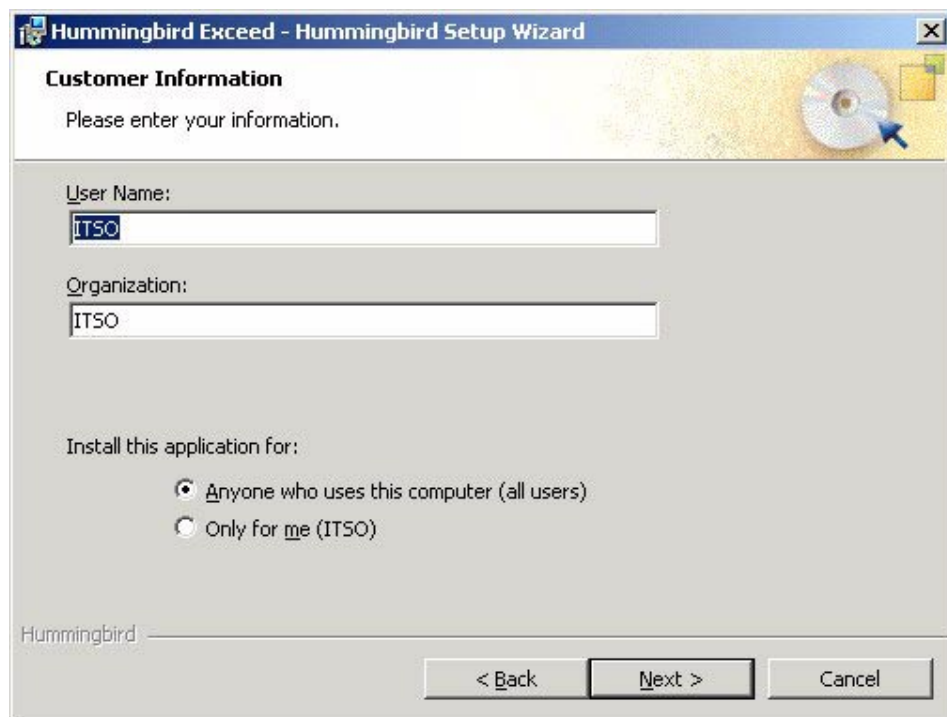


Figure 103. Exceed user name and security options

Fill in your user name and organization. Under those boxes are the options for application access. The first option allows for access to anyone logging into the particular system you are doing the install on, and the second option limits access only for the user ID you are specifying above.

After you are finished, click on **Next** and either change the installation path or accept the default installation path by clicking on **Next** again.

Next you will be presented the dialog box shown in Figure 104.

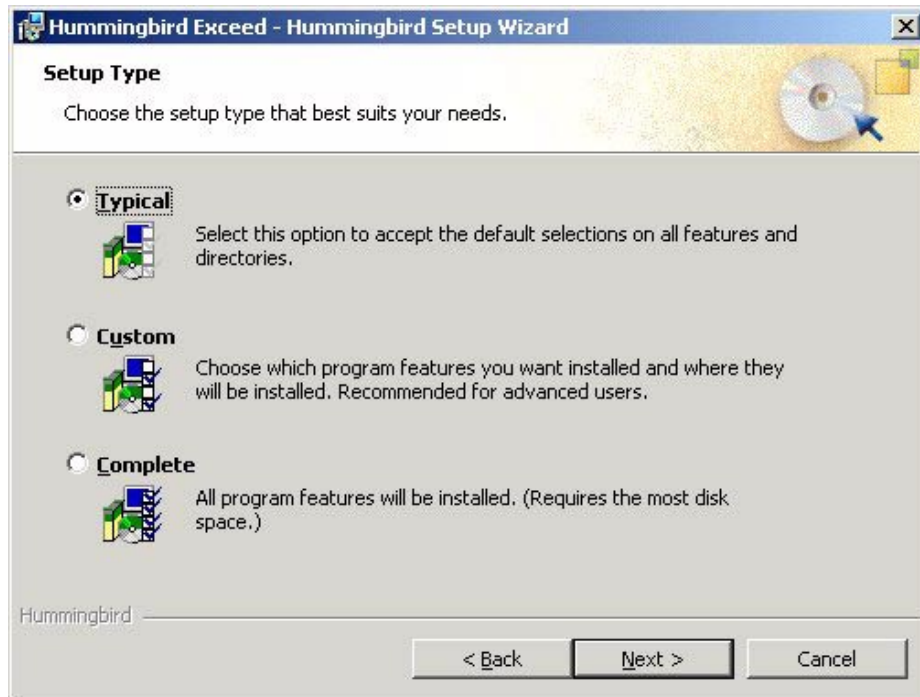


Figure 104. Exceed choose installation type

Click on **Next** to accept default settings for installation, choose **Custom** to selectively install Exceed components, or select **Complete** to install every available application component.

The next panel will give you the options of going back and changing installation settings by clicking on **Back**, or accepting all of the installation settings you have chosen and proceeding with the installation by clicking on **Install**.

Following the installation of application files, the Exceed installation should do a keyboard detection and prompt you to respond with your keyboard type. Click on **Next** and you will be given the dialog box shown in Figure 105 on page 186.



Figure 105. Exceed set password for Xconfig

Xconfig controls all communication and application settings for Exceed. You can either specify a password to protect all Xconfig settings and click on **Next**, or enter nothing and click on **Skip**.

Next you will be prompted on whether or not to tune the graphics settings for Exceed to emulate X Window CDE on your desktop, as shown in Figure 106 on page 187.



Figure 106. Exceed tune Xserver graphics settings

If you click on **Next** to proceed, the process might take up to eight minutes to complete. To avoid this process, click **Skip**.

After all this is completed, you should be shown a panel letting you know that the installation has completed. Click on **Finish** to complete the installation.

### 5.2.2 Exceed setup

To emulate the X Window CDE on your Windows desktop, you will have to configure Exceed to submit an X Window Display Manager (XDM) query to your AIX 5L system. Click on **Start -> Programs -> Hummingbird Connectivity 7.0 -> Exceed -> Xconfig** to bring up Xconfig for Exceed.

The panel displayed in Figure 107 on page 188 will appear.



Figure 107. Exceed starting Xconfig

Double click on the **Communication** icon to display the panel shown in Figure 108.

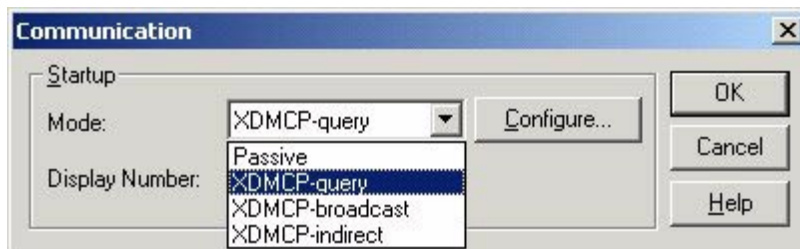


Figure 108. Exceed configure XDM

Click on the pull down panel, select **XDMCP-query**, and click on **Configure** to specify an XDM host. We are selecting **XDMCP-query** so that we can specify a specific IP address of the system we want to start a session on through the XDM. The XDMCP Startup Modes panel is displayed in Figure 109 on page 189.

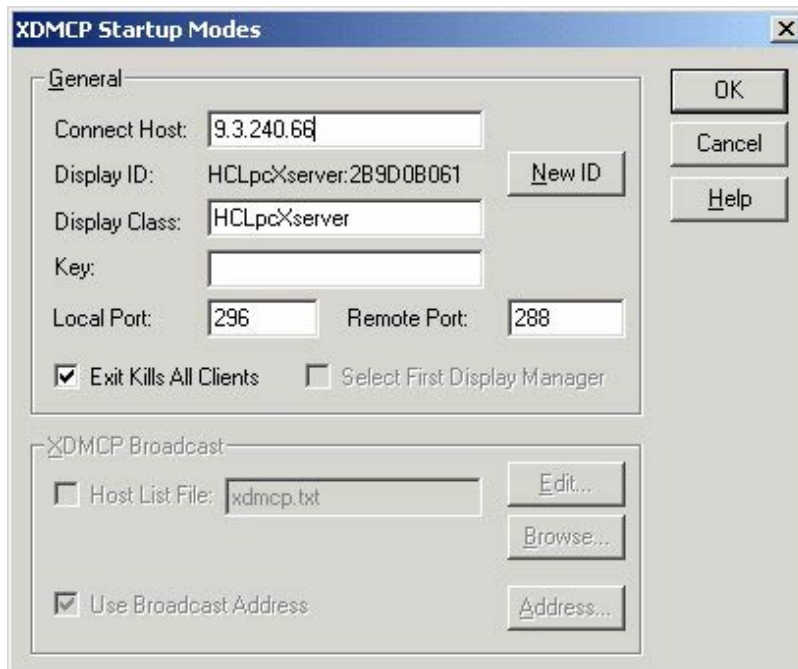


Figure 109. Exceed specify IP for XDM query

In the panel **Connect Host**, specify the IP address of the AIX 5L system you want to emulate and click on **OK**.

If the Exceed XServer was running in the background, Xconfig will then prompt you to restart the Exceed server, as shown in Figure 110. Click on **Yes** to restart Exceed. Doing this will submit a request to start an X Window terminal to the IP address specified above. Assuming the system at the IP address specified gets the query, it will be routed to the dtlogin process, which will in turn send data back to Exceed to generate an X Window desktop. Now you should be prompted to log in just as if you were seated at your AIX 5L system.

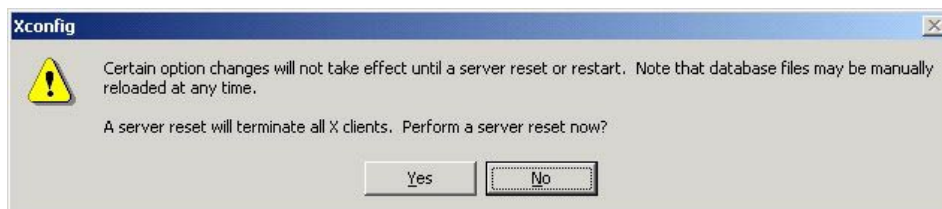


Figure 110. Exceed restart server for XDM

There are two main ways to bring up an XDM client session:

- For advanced connections, click on **Start -> Programs -> Hummingbird Connectivity 7.0 -> Exceed -> Xsession**, which will bring up the panel shown in Figure 111. This will submit an XDMCP broadcast and give you a panel showing you all systems on the network that will allow you to start an X Window session on your system.

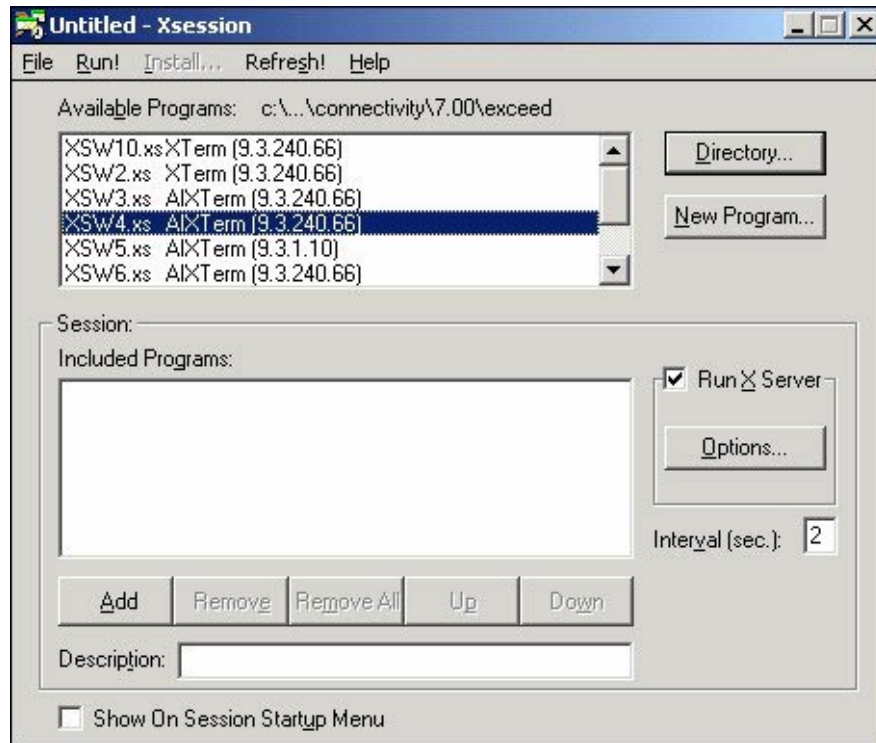


Figure 111. Exceed start XDM client

Click on the host you would like to connect to and then click on **Run!** to begin your XDM client session. This method is good if the user wants to create an icon for each of his/her XDMCP-query sessions on the desktop. This way, they can simply click that icon on their Windows desktop the next time they want to launch a UNIX desktop.



### Note

To completely restart your XDM client session, log out of the X Window CDE and then right-click on the Exceed entry on your task bar. Click on **Close** and then answer **Yes** when it asks you if you want to shut down your X Window session. Or click the red stop icon in the Exceed toolbar. It will ask "This will end your X Window session." Click **OK** to end the Xserver.

- Another way to start an XDM client session is to bring up the X Window Display Manager Control Protocol (XDMCP) Manager Chooser. Click on **Start -> Programs -> Hummingbird Connectivity 7.0 -> Exceed -> Exceed (XDMCP-Broadcast)** icon (the gold X with the black top hat). This will launch your preconfigured XDMCP Query Session, as shown in Figure 112. For easier access, this icon can be copied to your desktop.

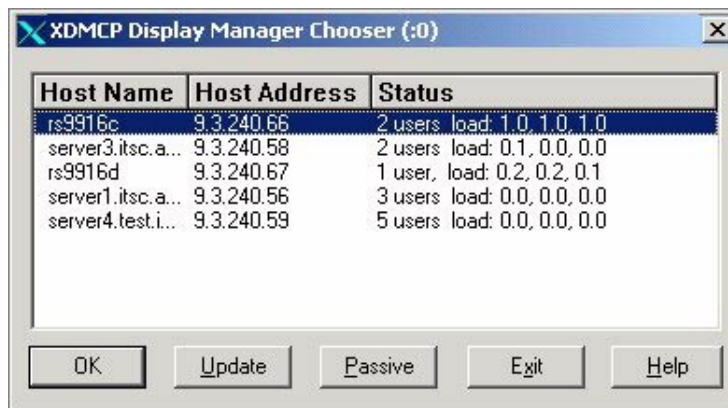


Figure 112. Exceed XDM broadcast panel

This is another panel that shows us all the systems on the local network available to us to start an XDM session with. Choose a server address and then click **OK** to begin an XDM client session with that system. To see what X Window might look like running on your system using Exceed, see Figure 127 on page 205.

## 5.3 Network Computing Devices PC-Xware

PC-Xware is a product from Network Computing Devices (NCD) Incorporated that, among other things, allows a client to emulate the CDE X Window environment from AIX 5L on their Windows workstation or server.

The prerequisites for this section are that you have both a functional Windows 2000 system and a functional pSeries system running AIX 5L, and that both systems can communicate normally over a TCP/IP network.

### 5.3.1 PC-Xware installation

In this section we are going to discuss the acquisition and installation of a trial version of PC-Xware software from NCD. For a full version of the product, you can visit NCD's Web site at:

<http://www.ncd.com>

At the time of writing, the standard trial versions of PC-Xware available from <http://www.ncd.com/products/software/pcxware/pcxeval.html> will not provide a version of the product compatible with Windows 2000. You will need to visit that site in order to get evaluation codes from NCD. Fill out the form available there and click on **Send**. Shortly afterwards, you should receive an e-mail that contains your serial number and authorization code, which will allow you to install and run a trial version of the software.

The version compatible with Windows 2000 is 5.01 D, and you will have to visit NCD's FTP site at <ftp.ncd.com> or [aphrodite.ncd.com](http://aphrodite.ncd.com) to obtain an evaluation copy. Once you have connected to their ftp server, specify your user name as anonymous and your password as your e-mail address. The file `pcx2000.exe` can be found in the directory `/pub/pcx/Archive/pcxware5.x/win2000/`.

Once the file is in a temporary directory, execute it, and you will get the dialog box shown in Figure 113.

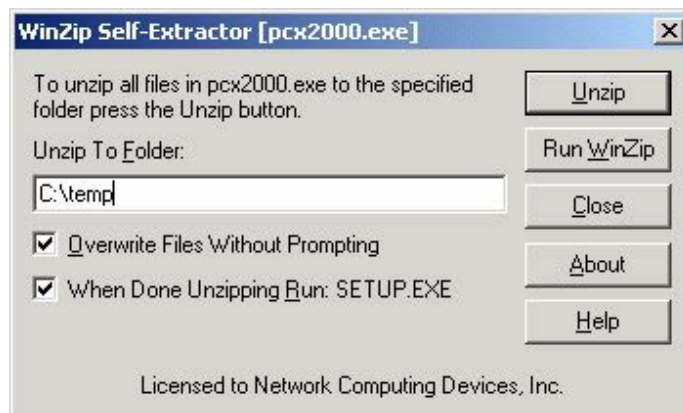


Figure 113. PC-Xware archive extraction

Specify a temporary directory, such as C:\temp. The check box for 'When Done Unzipping Run: SETUP.EXE' should already be filled in.

Once extraction is complete, SETUP.EXE should execute automatically, and you will be presented with the dialog box shown in Figure 114.

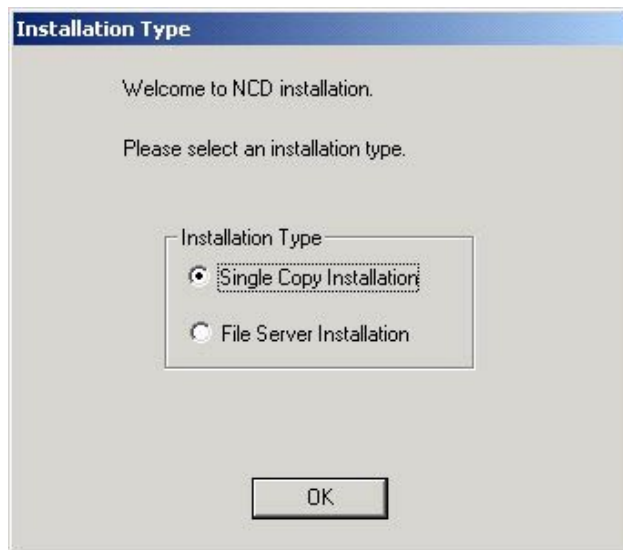


Figure 114. PC-Xware installation type

Specify **Single Copy Installation** and then click the **OK** button.

Before this point, you should have been contacted by an NCD support technician with your serial number and authorization code for the evaluation copy of the software off the FTP site. From the e-mail you received from them, fill in the Serial Number and Authorization Code fields with the information provided to you by NCD. The dialog box for this step is shown in Figure 115 on page 194.



Figure 115. PC-Xware registration information

After you have filled in your evaluation codes, you will be prompted for a permanent directory for PC-Xware to be installed into. This dialog box is presented in Figure 116.

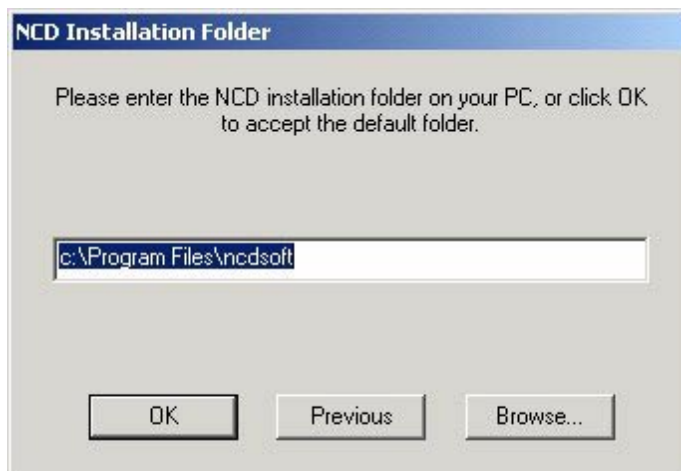


Figure 116. PC-Xware installation path

After providing an installation path, SETUP.EXE will extract all the files necessary for PC-Xware to run properly. When this is finished, you should be presented with the data in Notepad shown in the next screen.

NCD Installation Information

\*\*\* PC-Xware \*\*\*

PC-Xware will be started after you reboot.

\*\*\* Un-Install \*\*\*

To Un-Install: please see "Removing an Installation" in the install and Configuration Guide.

Installation Complete

Shut down all open applications and restart your computer. After you have logged into your system, you will be able to begin using PC-Xware.

### 5.3.2 PC-Xware configuration

To create an X Window Display Manager (XDM) session within PC-Xware, click on **Start -> Programs -> NCD PC-Xware -> PC-Xware Connection Wizard**. You will then be presented with the dialog box shown in Figure 117.

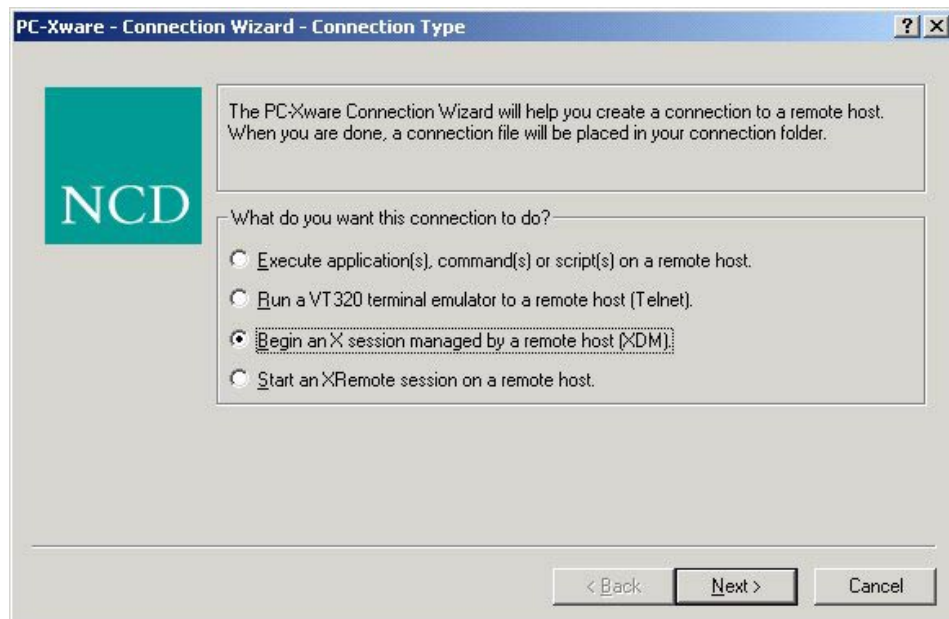


Figure 117. PC-Xware configure XDM session

Select the radio button for **Begin an X session managed by a remote host (XDM)** and click on the **Next** button. You will get the dialog box shown in Figure 118 on page 196.

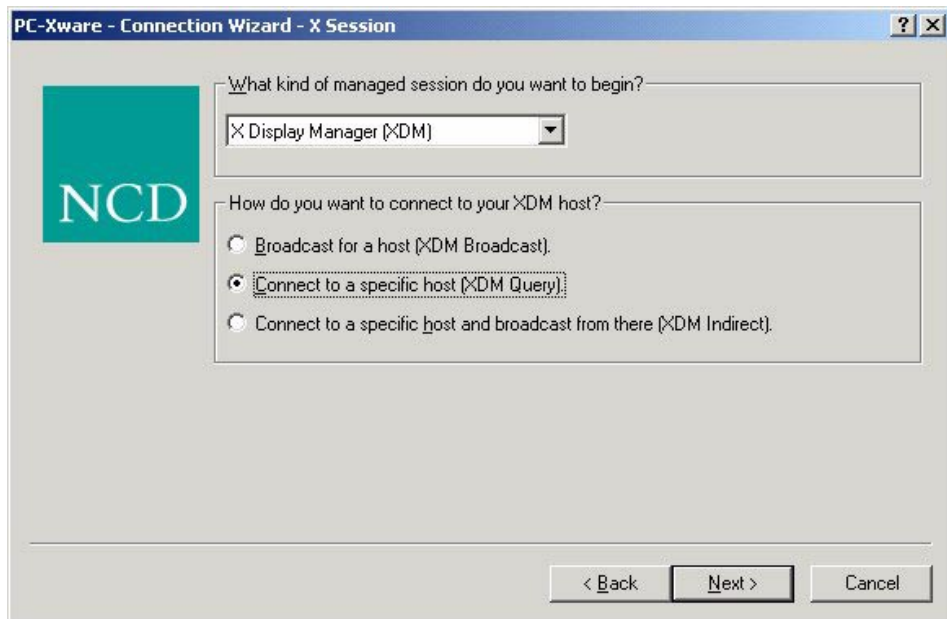


Figure 118. PC-Xware specify XDM type

Select the radio button **Connect to a specific host (XDM Query)**. Using this configuration setting will allow you to specify the IP address of the RS/6000 host you want to connect to, as seen in Figure 119 on page 197. After specifying the IP address, click on **Next**.

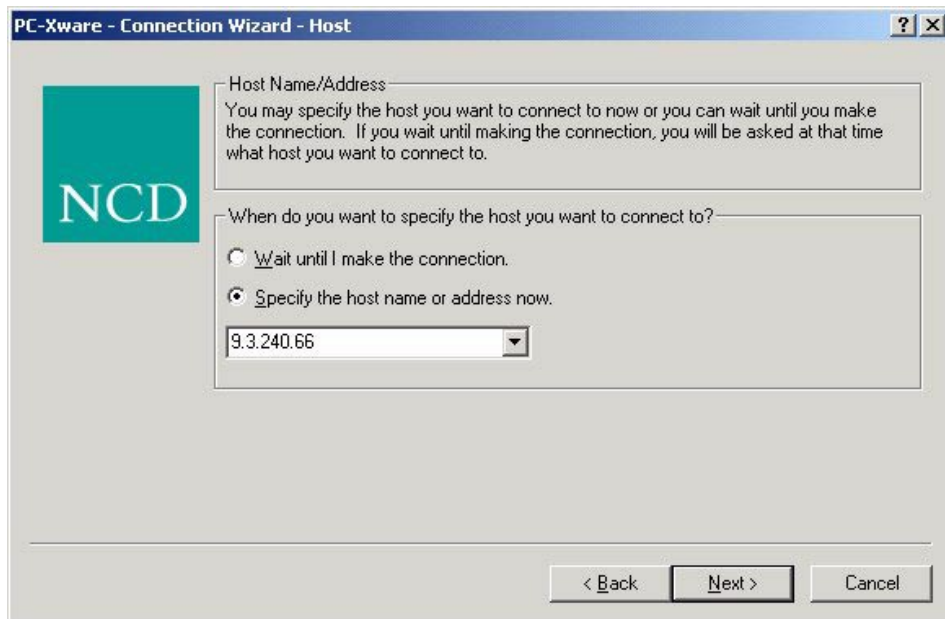


Figure 119. PC-Xware specify IP address

In the next dialog box, shown in Figure 120 on page 198, you will be prompted to name the startup icon for the settings you have just specified. After you are done, click **Finish**.

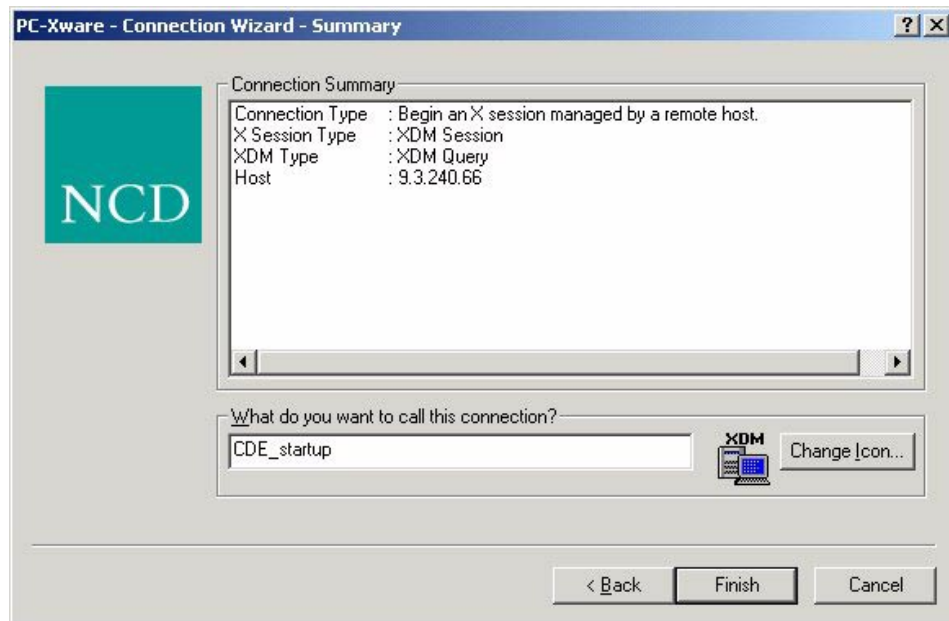


Figure 120. PC-Xware specify name for icon

Next, click on **Start -> Programs -> NCD PC-Xware -> PC-Xware Connections**. This will bring up the panel that will show you the newly created icon for your connection.

---

## 5.4 WRQ's Reflection

Reflection is yet another product available for Windows 2000 that allows you to use X Window applications on your Windows 2000 desktop. Reflection 8.0 offers terminal emulation not only for Xterm and AIXterm, but also for other UNIX terminals, as well as full support for XDMCP and XDM communication. More information on their product is available at:

[http://www.wrq.com/products/reflection/pc\\_unix/](http://www.wrq.com/products/reflection/pc_unix/)

After you have either obtained and installed a full version of the product or a trial version, click on **Start -> Programs -> Reflection -> Reflection X** to bring up the panel shown in Figure 121 on page 199.



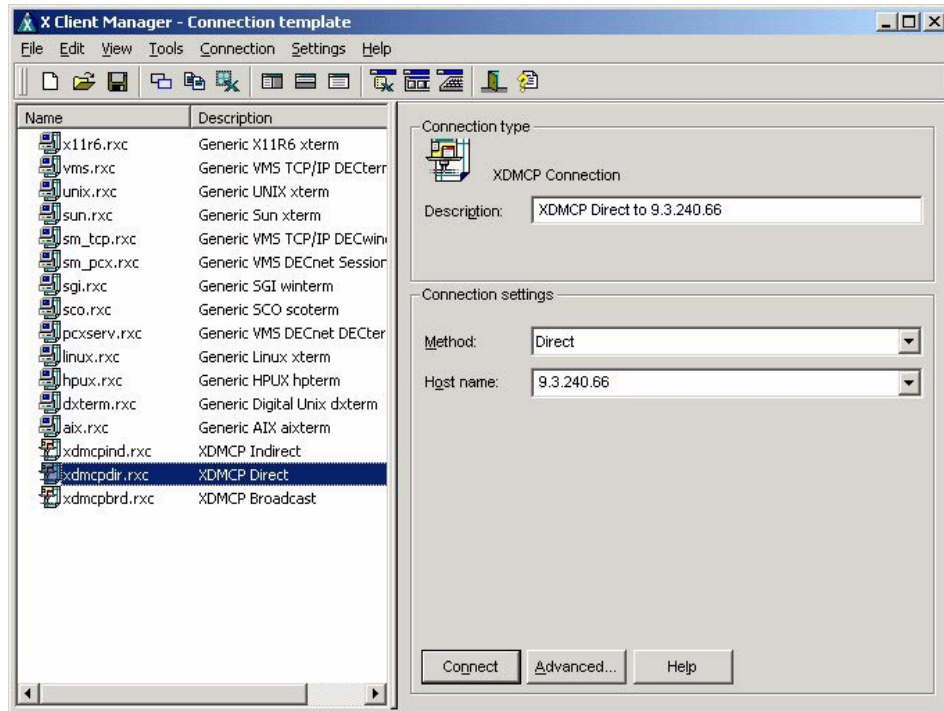


Figure 121. Reflection X startup panel

Figure 121 shows a selection for Reflection to start an XDM session with 9.3.240.66. First click on **XDMCP Direct**, click on **Host name**, fill out the IP address or DNS entry of the server you want an X Window session from, and then click on **Connect** to begin an XDM session with the server.

Like Exceed and PC-Xware, Reflection 8.0 can be configured to start up a standard xterm, as seen in Figure 122 on page 200.

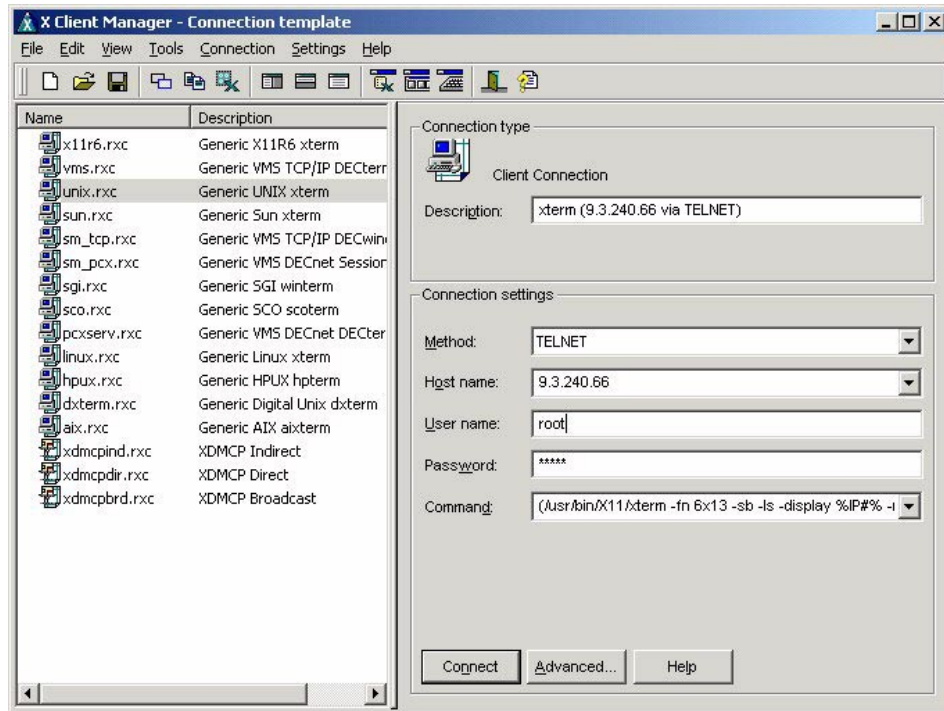


Figure 122. Reflection xterm startup panel

Using a similar procedure to the one followed for Figure 121 on page 199, we again fill out the host name, but also have the option of providing our user name and password for the session we want to create.

---

## 5.5 Using XDM client software for interoperability solutions

In this section, we will show how these three solutions function with the Windows 2000 desktop.

### 5.5.1 Exceed functionality

The same result can be achieved in different ways with Hummingbird Exceed. If you go into Xconfig, as shown in Section 5.2.2, “Exceed setup” on page 187, double-click on the Communication icon, and then choose **Passive** instead of **XDMCP-query**. Exceed will then start in a passive mode instead of active and will only execute an XDM session if you request one, not upon starting Exceed.

On your AIX system, type `export DISPLAY=your IP address:0` (where your IP address is your IP address) to let AIX know to send the X Window output to your Windows 2000 system. Next, start an application like xterm from your AIX 5L system, and you should get an output similar to that seen in Figure 124 on page 202.

Also, you can use the client wizard, available through **Start -> Programs -> Hummingbird Connectivity 7.0 -> Exceed -> Client Wizard**, to configure xterm icons for specific hosts. After you have gone through the process of adding xterm sessions within Exceed, you can click on **Start -> Programs -> Hummingbird Connectivity 7.0 -> Exceed -> Exceed**, which starts Exceed in Passive mode. Right-click on the Exceed icon in your task bars, and then hold the mouse over **Tools**. Under **Client Startup**, you will see any xterms you created using the Client Wizard, and you can start them. An xterm started through Exceed will look similar to the one in Figure 124 on page 202.

Figure 123 shows the Exceed Toolbar, which provides copy and paste capabilities, access to different Exceed applications, a customizable desktop, a function to stop the Xserver, and more. This toolbar is customizable by the user.

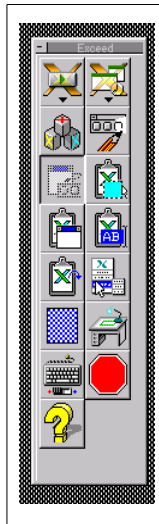


Figure 123. Exceed toolbar

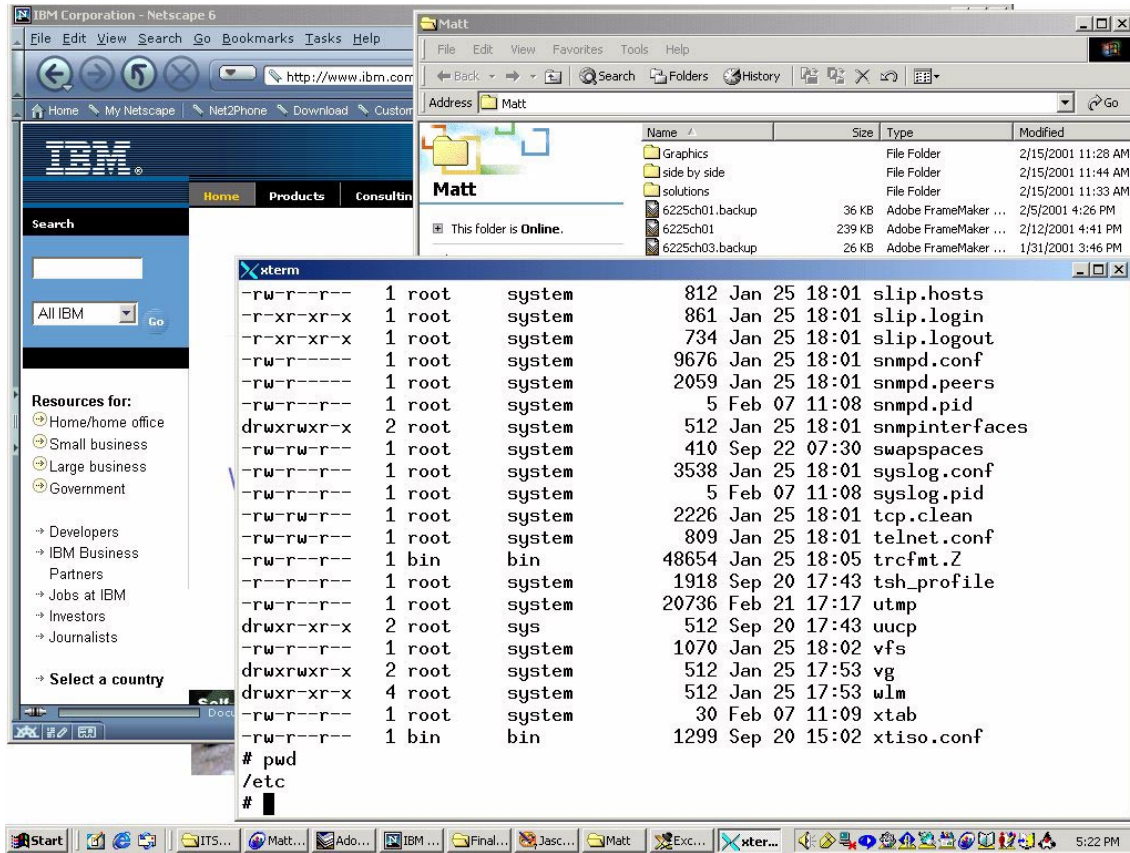


Figure 124. Exceed xterm exported to Windows desktop

The process described for exporting an xterm to a Windows desktop using PC-Xware will work for Exceed if you have Exceed running in passive mode. It will open a panel similar to the one shown in Figure 125 on page 203.

### 5.5.2 PC-Xware functionality

With NCD's PC-Xware running, you can export any single graphical panel to your desktop. On your AIX system, type `export DISPLAY=your IP address:0` (where `your IP address` is your IP address) to let AIX know to send the X Window output to your Windows 2000 system. Next, start an application like xterm from your AIX 5L system; you should get an output similar to that seen in Figure 125 on page 203.

The same result can be achieved just by using the PC-Xware Connection Wizard. Just click on **Start -> Programs -> NCD PC-Xware -> PC-Xware**

**Connection Wizard** and configure an xterm session icon for PC-Xware. The results of this will be similar to Figure 125.

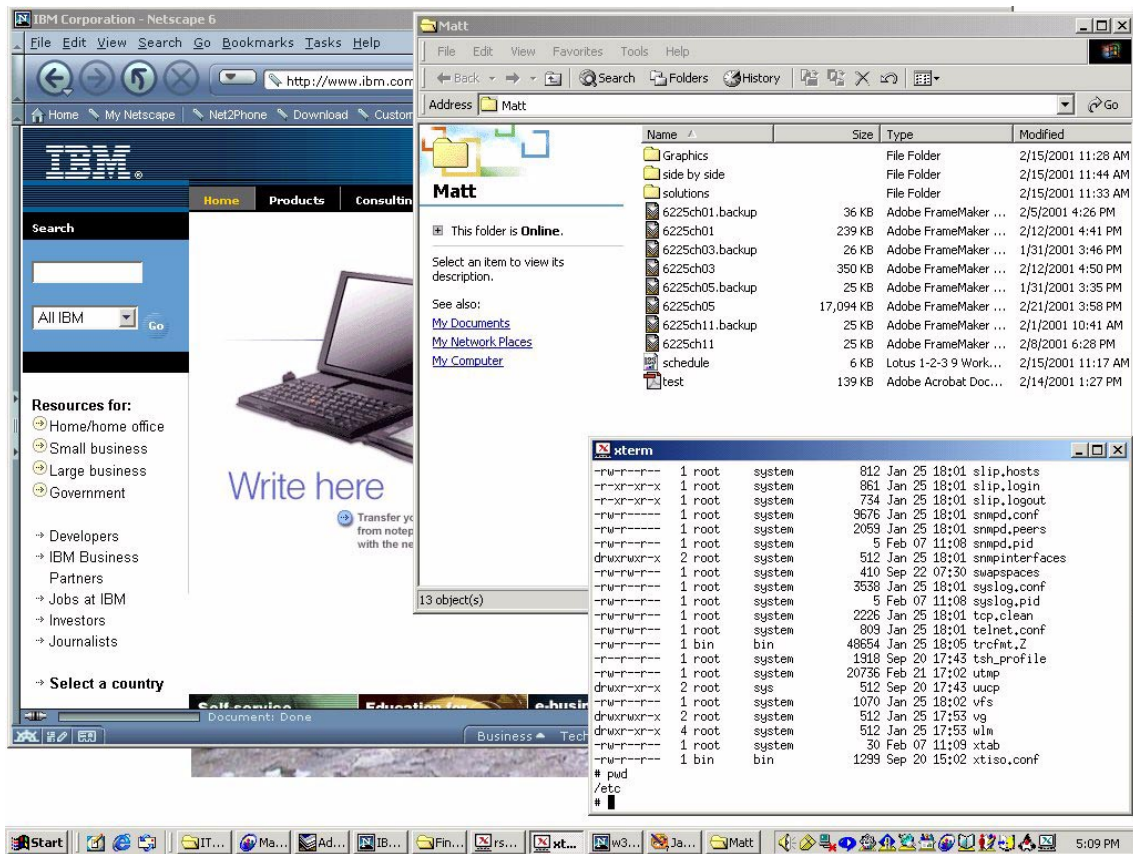


Figure 125. PC-Xware xterm session exported to Windows desktop

### 5.5.3 Reflection functionality

As with Exceed (Section 5.5.1, “Exceed functionality” on page 200) and PC-Xware (Section 5.5.2, “PC-Xware functionality” on page 202), Reflection can also accept an exported display, and an xterm can be started up normally just by using the Reflection X Client Manager (Figure 122 on page 200). A xterm brought up either way might appear as in Figure 126 on page 204.

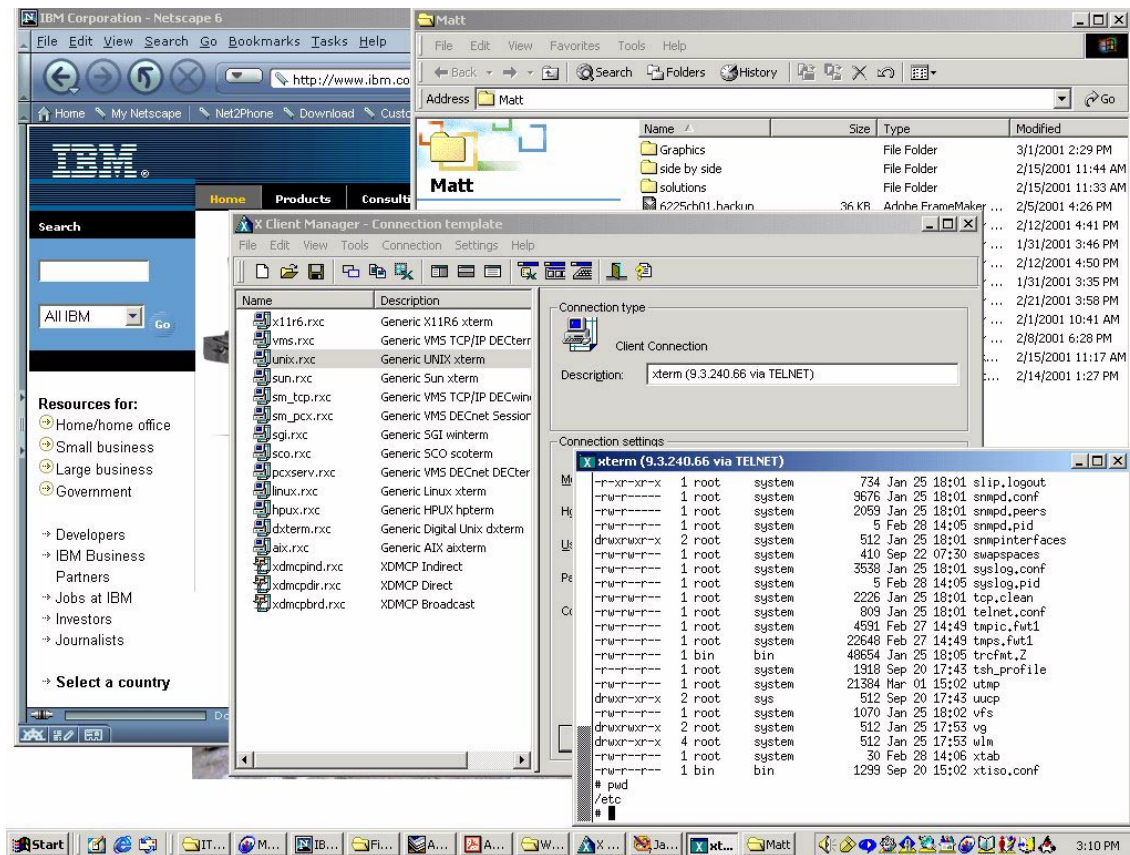


Figure 126. Reflection export an xterm session

### 5.5.4 Full X Window export to Windows desktop

Using either Hummingbird Exceed, NCD's PC-Xware, or WRQ's Reflection to start an XDM client and emulate the X Window CDE on your Windows desktop, you will be prompted to specify a user ID and password, just as if you were at the terminal where AIX 5L is running on your system.

After providing your user ID and password, your desktop will look similar to Figure 127 on page 205. As you can see, using an XDM client to emulate the CDE on our Windows desktop allows us to have both X Window and Microsoft Windows open at the same time, and to go between folders and applications running on both systems.

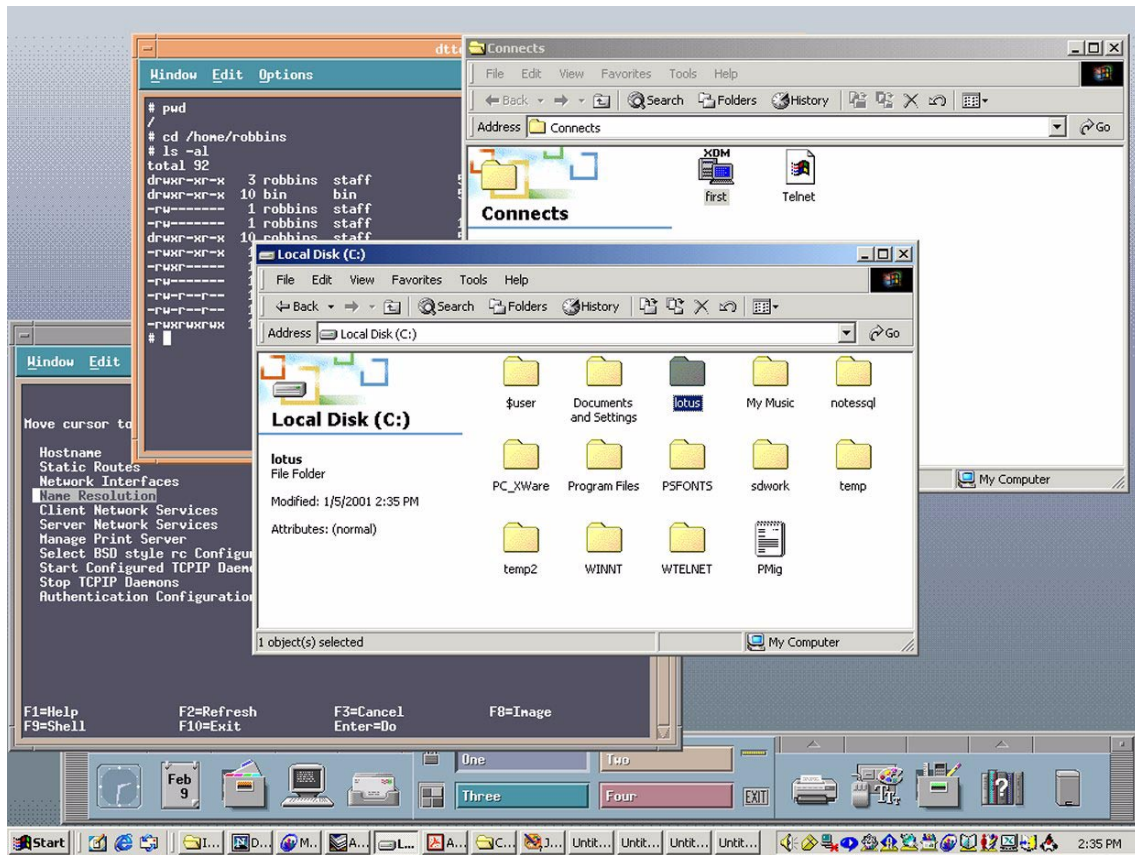


Figure 127. CDE and Windows 2000 working together

Furthermore, as can be seen in Figure 128 on page 206, we can cut and paste text between Windows and X Window applications, such as Lotus Notes and vi.

Large pSeries systems are often stored in raised floor areas and kept in system racks due to their cooling and power requirements. Being able to go between your Intel system and pSeries system without having to leave your desk can achieve a great deal towards helping you install and use solutions on both systems more efficiently.

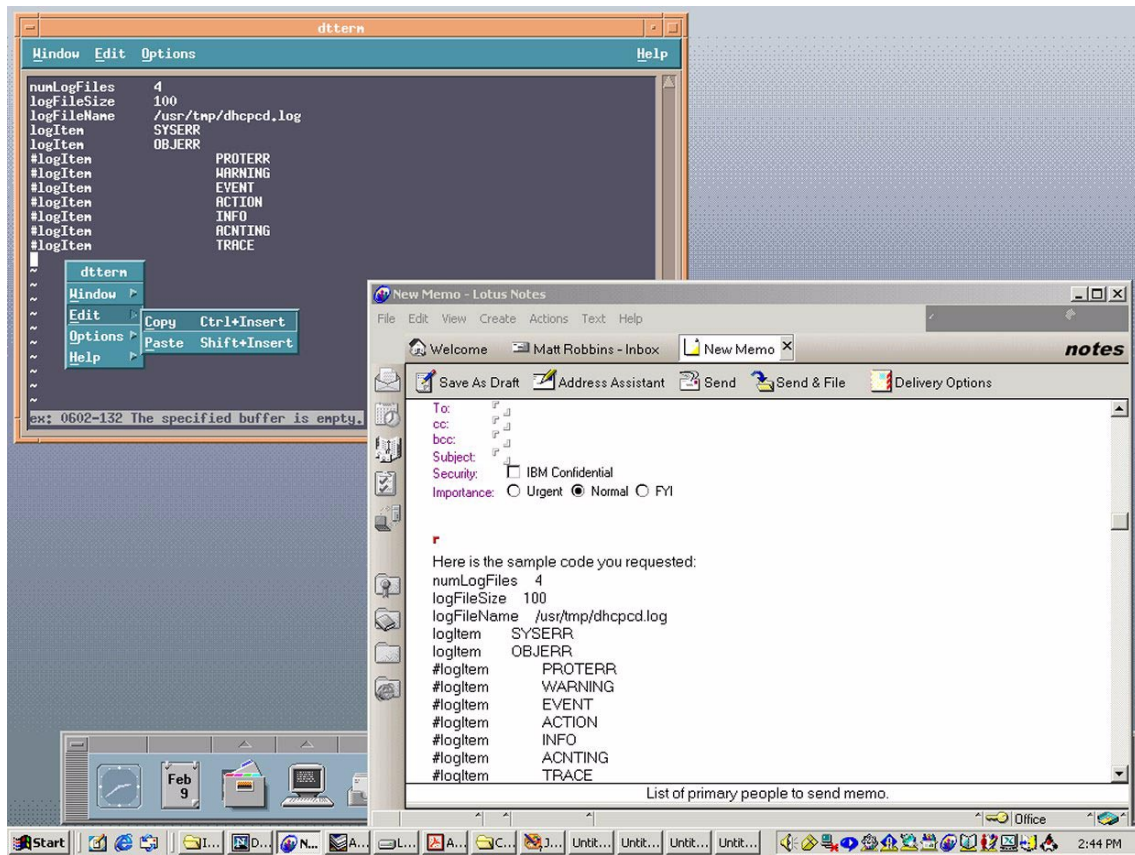


Figure 128. Cutting and pasting between X Windows and Windows applications

When setting up AIX Fast Connect or Samba, you could use PC-Xware to set up the storage and networking solution on the AIX side, and then switch to the client side to configure network storage for your Windows system on the AIX system. In using SFU, you could create an NFS file system on your Windows server and then test it out and use it from the AIX side just by switching over to the XDM.

While most of these tasks can be provided over a telnet session on the network, more and more services are being added to AIX that use a graphical interface. These solutions allow you to take advantage of the latest user interfaces without having to physically be at your AIX 5L system.



---

## 5.6 Citrix MetaFrame

This section will discuss the MetaFrame product from Citrix Systems Inc. and how it can help integrate your AIX 5L and Windows 2000 environments.

Founded in 1989, Citrix Systems, Inc. develops application server software and services that offer the ability to run any application on any device over any connection using the proprietary ICA (Independent Computing Architecture) protocol.

### 5.6.1 Overview

Citrix MetaFrame is a server-based computing software for Microsoft Windows 2000/NT4 TSE and UNIX. MetaFrame delivers a comprehensive solution to the enterprise by extending graphical end-user applications from a central server to various heterogeneous computing environments.

On Windows servers, MetaFrame adds additional client and server functionality to the Terminal Services, including support for non-Windows clients. UNIX Servers will benefit from ICA connectivity on top of the X Window or CDE Window managers.

#### 5.6.1.1 The ICA concept

As part of the core MetaFrame architecture, the ICA components make the whole concept possible. The ICA technology consists of a server software component, a network protocol component, and a client software component working together to create one of the most flexible computing architectures available.

On the MetaFrame server, the ICA component separates the application logic from the user interface, efficiently transporting only the changes necessary to the ICA network protocol for further transportation over LAN or WAN links using any of the TCP/IP, IPX, or NetBEUI network protocols. The concept of transporting only panel changes necessary is illustrated in Figure 129 on page 208 (from the Citrix Web site).

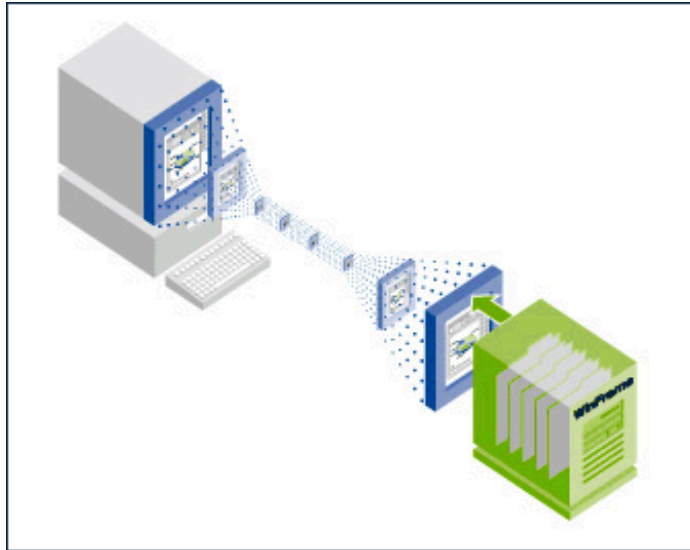


Figure 129. User interface transportation over ICA

The ICA network protocol transports keystrokes, mouse clicks, and panel updates to the client, requiring less than 10 Kbs bandwidth for low impact applications. Heavy graphic applications will, of course, require more bandwidth to run smoothly, but using sophisticated caching techniques keeps the demand for bandwidth to a minimum. Figure 130 (also from the Citrix Web site) shows the bandwidth of some common media relative to the ICA protocol stream.

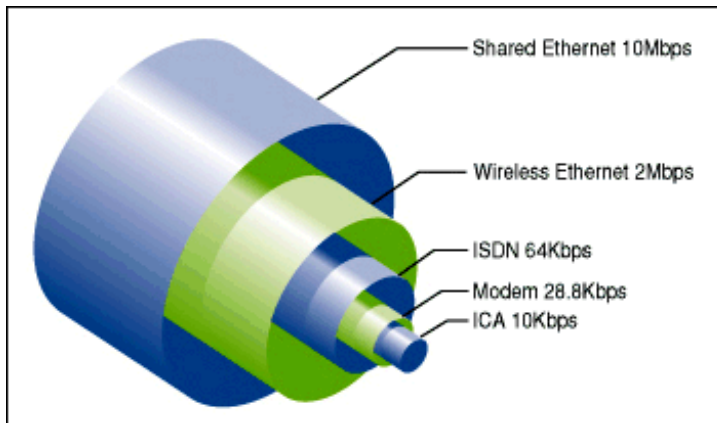


Figure 130. ICA bandwidth consumption

On the client, users work with the application's interface as if it was installed locally on the client, sending keystrokes and mouse clicks over the network and receiving panel updates from the server.

Even between AIX machines, using ICA connections instead of X.11 connections can save considerable amounts of network bandwidth because the average bandwidth required by X.11 is between 15 and 25 times greater than the bandwidth required by ICA.

At time of writing, ICA clients are available for the following operating systems:

- Microsoft DOS/Windows
  - DOS16
  - DOS32
  - Win16
  - Win32
  - Windows CE
    - x86
    - SH3
    - SH4
    - MIPS
    - PPC
    - ARM
- OS/2 Warp
- Apple Macintosh
- EPOC32
- UNIX
  - AIX
  - Solaris
    - Sparc
    - x86
  - SunOS
  - Tru64
  - HPUX
  - IRIX
  - Linux
    - x86
    - ARM
  - SCO
- Java
- ActiveX

### **SecureICA**

Citrix SecureICA Services enhances the security of MetaFrame by allowing users to access Citrix servers over secure communications channels.

The MetaFrame server and ICA client use the Diffie-Hellman key agreement algorithm with a 1024-bit key to generate the RC5 keys used for encryption. Each connection uses a unique, random key pair, and a system service periodically generates new Diffie-Hellman parameters in the background, providing an enhanced level of security. SecureICA encryption is applied to the entire ICA packet except for a small encryption header.

The encryption algorithms used by SecureICA are highly optimized, imposing an almost negligible performance impact on the ICA client.

SecureICA is a feature only available on MetaFrame for Window 2000 and Windows NT4.

## **5.6.2 MetaFrame for AIX**

MetaFrame for AIX adds the ICA functionality to the X Window/CDE environment, allowing you to connect to AIX MetaFrame servers using an ICA client. Combined with MetaFrame for Windows 2000 (discussed in Section 5.6.3, “MetaFrame for Windows 2000” on page 221), your user environment will be very coherent and easy to manage. MetaFrame for AIX supports AIX Version 4.3.3 and above.

### **5.6.2.1 MetaFrame for AIX installation**

This section will describe how to install Citrix MetaFrame for AIX Version 1.1 using SMIT.

#### **Note**

You have to be logged in as root in order to successfully complete the following steps.

MetaFrame for AIX uses the `ctxsrvr` user and the `ctxadm` group to set up daemons and security, so we have to start the installation by creating these two accounts using the `mkuser` and `mkgroup` commands. Feel free to use SMIT to create the accounts if you prefer:

```
# mkuser ctxsrvr
# mkgroup ctxadm
```

After successfully creating the user and the group, use SMIT to install the application. Start SMIT using the `installp` fastpath:

```
# smitty installp
```

This will bring up the 'Install and Update Software' screen. Select 'Install Software' by pressing Enter to bring up the 'Install Software' screen. Select the directory or device you will use for installation. In this case, we choose /dev/cd0, which is the CD-ROM.

```

                                Install Software

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

                                [Entry Fields]
* INPUT device / directory for software      /dev/cd0
* SOFTWARE to install                       [_all_latest]      +
PREVIEW only? (install operation will NOT occur)  no                +
COMMIT software updates?                    yes               +
SAVE replaced files?                        no                +
AUTOMATICALLY install requisite software?      yes               +
EXTEND file systems if space needed?          yes               +
OVERWRITE same or newer versions?            no                +
VERIFY install and check file sizes?         no                +
Include corresponding LANGUAGE filesets?      yes               +
DETAILED output?                            no                +
Process multiple volumes?                   yes               +
ACCEPT new license agreements?              no                +
Preview new LICENSE agreements?              no                +

F1=Help          F2=Refresh      F3=Cancel      F4=List
Esc+5=Reset      F6=Command    F7=Edit       F8=Image
F9=Shell        F10=Exit     Enter=Do
```

Move the cursor to the 'SOFTWARE to install' field and press F4 for a list of available applications in the directory or on the media you have selected. The list should look similar to the following screen.

```
SOFTWARE to install

Move cursor to desired item and press F7. Use arrow keys to scroll.
ONE OR MORE items can be selected.
Press Enter AFTER making all selections.

[MORE...4]
#
#-----
> Citrix.MetaFrame ALL
  1.1.0.0 MetaFrame for Unix
  1.1.0.0 MetaFrame for Unix anonymous user setup
  1.1.0.0 MetaFrame for Unix automatically shutdown/start on system
  1.1.0.0 MetaFrame for Unix manual pages
[BOTTOM]

F1=Help           F2=Refresh       F3=Cancel
F7=Select         F8=Image         F10=Exit
Enter=Do          /=Find          n=Find Next
```

Move the cursor to the line reading 'Citrix.MetaFrame' and press F7 to select all of the four available packages, then press Enter to return to the 'Install Software' screen.

Press Enter to start the installation, and Enter again to confirm the 'Are you sure?' dialog.

After the installation is finished, make sure it reads OK (the Command: OK should be visible in the upper left corner), and that it looks similar to the following screen.



The final installation step is to add a MetaFrame license key to the server so it starts serving login requests. Because we added the path to the MetaFrame commands, you should be able to issue the following command from anywhere. If not, change directory to /usr/lpp/CTXSmf/sbin before doing so.

```
# ctxlicense -add EUL-0634-9F36-XXXX-000167
Citrix license EUL-0634-9F36-XXXX-000167-YYYY-0584
has been successfully added.
```

You need to activate this license within 2 days. If the license is not activated during this time, it will no longer allow user connections.

Use the Citrix Web site (<http://www.citrix.com/activate/login.htm>) to activate your license. Enter the activation code using the `ctxlicense` command again as follows:

```
# ctxlicense -activate <license number> <activation code>
```

This concludes the installation.

### **Feature Release 1**

Feature Release 1 is an add-on to MetaFrame that adds the following functionality:

<b>Increased Color Depth</b>	Support for up to 24 bit color depths (instead of 8 bit)
<b>Increased Video Resolution</b>	Support for screen resolutions up to 32,767 x 32,767 pixels
<b>Multi-Monitor Support</b>	Support for client devices with multiple monitors

#### **Note**

At the time of writing, we have accessed the Early Access Version of Feature Release 1 for MetaFrame for AIX. All screenshots are for Early Access Version of Feature Release 1, and may change when the full version is available. The final version will add SSL encryption of ICA and NFuse traffic, Client Drive Mapping, and various other enhancements, as described in “Feature Release 1” on page 222.

For convenience, we will use the `ctxsrvr` user account in the following example and `su` to root when needed. Before we start the installation, we need to stop the MetaFrame server using the `ctxsrvr` command:



```
$ ctxsrv stop all
Copyright 1999-2000 Citrix Systems, Inc. All Rights Reserved.
ctxibrowser stopped OK
Copyright 1999-2000 Citrix Systems, Inc. All Rights Reserved.
ctxfm stopped OK
```

If you have users running on your system, you could use the `ctxshutdown` command instead, adding a message to your users that the server will be brought down. An example of this is shown in the following screen, using the default time-out of 60 seconds.

```
$ ctxshutdown "Server will be brought down for maintenance. Please log
ctxshutdown: Locking the server from accepting further logins.
ctxshutdown: Locked server against further logins.
ctxshutdown: Active sessions: 1
ctxshutdown: Found some active sessions. Informing them of shutdown.
Successfully sent message to session ID: 1.
ctxshutdown: Told session '1'
ctxshutdown: Waiting for 60 seconds...
ctxshutdown: done.
ctxshutdown: Found some outstanding sessions. Auto-logging-off 1 .
ctxshutdown: Auto-logoff sent to session '1'.
ctxshutdown: Waiting for 30 seconds...
ctxshutdown: done.
ctxshutdown: Killing those remaining and killing MetaFrame server.
Copyright 1999-2001 Citrix Systems, Inc. All Rights Reserved.
ctxibrowser stopped OK
Copyright 1999-2001 Citrix Systems, Inc. All Rights Reserved.
ctxfm stopped OK
ctxshutdown: Shut down the MetaFrame server.
ctxshutdown: All sessions successfully shutdown.
```

With MetaFrame shut down, we can start the installation. This requires root access rights, so we have to `su` to root before we start the installation process:

```
$ su -
root's Password:
# smitty installp
```

Select 'Install Software' from the 'Install and Update Software' screen by pressing Enter. The 'Install Software' screen will appear. Select the directory or device you will use for installation. In this case, we choose `/tmp/fr1`, because we have the installation code in this directory.

Move the cursor to the 'SOFTWARE to install' field and press F4 for a list of available applications in the directory or on the media you have selected, which should look similar to the following screen.

```

SOFTWARE to install

Move cursor to desired item and press F7. Use arrow keys to scroll.
ONE OR MORE items can be selected.
Press Enter AFTER making all selections.

[MORE...4]
#
#-----
> Citrix.MetaFrame                                ALL
  1.1.1.0 MetaFrame for Unix
  1.1.1.0 MetaFrame for Unix anonymous user setup
  1.1.1.0 MetaFrame for Unix automatically shutdown/start on system
  1.1.1.0 MetaFrame for Unix manual pages
[BOTTOM]

F1=Help          F2=Refresh      F3=Cancel
F7=Select        F8=Image        F10=Exit
Enter=Do         /=Find         n=Find Next

```

Move the cursor to the line reading 'Citrix.MetaFrame' and press F7 to select all of the four available packages, then press Enter to return to the 'Install Software' screen.

Move the cursor to the 'COMMIT software updates' field and press Tab to change this from the default 'yes' to 'no'. If you keep the default setting of 'yes,' you will not be able to uninstall Feature Release 1 at a later time. The following screen shows this operation.

```

                                Install Software

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

                                [Entry Fields]
* INPUT device / directory for software      /tmp/fr1
* SOFTWARE to install                       [Citrix.MetaFrame   > +
  PREVIEW only? (install operation will NOT occur)  no                +
  COMMIT software updates?                       no                +
  SAVE replaced files?                           no                +
  AUTOMATICALLY install requisite software?       yes               +
  EXTEND file systems if space needed?            yes               +
  OVERWRITE same or newer versions?               no                +
  VERIFY install and check file sizes?           no                +
  Include corresponding LANGUAGE filesets?        yes               +
  DETAILED output?                                no                +
  Process multiple volumes?                       yes               +
  ACCEPT new license agreements?                  no                +
  Preview new LICENSE agreements?                 no                +

F1=Help           F2=Refresh           F3=Cancel           F4=List
Esc+5=Reset       F6=Command           F7=Edit            F8=Image
F9=Shell          F10=Exit             Enter=Do

```

Press Enter to start the installation, and Enter again to confirm the installation. After completing the installation, you should see a screen similar to the following screen.

```

                                COMMAND STATUS

Command: OK           stdout: yes           stderr: no

Before command completion, additional instructions may appear below.

[MORE...91]

Installation Summary
-----
Name                    Level           Part            Event           Result
-----
Citrix.MetaFrame.rte    1.1.1.0        USR             APPLY           SUCCESS
Citrix.MetaFrame.boot   1.1.1.0        USR             APPLY           SUCCESS
Citrix.MetaFrame.anon   1.1.1.0        USR             APPLY           SUCCESS
Citrix.MetaFrame.man    1.1.1.0        USR             APPLY           SUCCESS

[BOTTOM]

F1=Help           F2=Refresh           F3=Cancel           Esc+6=Command
Esc+8=Image       Esc+9=Shell          Esc+0=Exit          /=Find
n=Find Next

```

Again, after the installation is finished, make sure it reads OK (the Command: OK should be visible in the upper left corner), as in the previous screen.

Finally, we have to start the MetaFrame services again using the `ctxsrv` command. For proper operation, exit from the root shell before starting the services, as seen in the following example:

```
# exit
$ ctxsrv start all
Copyright 1999-2001 Citrix Systems, Inc. All Rights Reserved.
ctxfm started OK
Copyright 1999-2001 Citrix Systems, Inc. All Rights Reserved.
ctxibrowser started OK
```

### 5.6.2.2 ICA Client installation on AIX

An ICA Client allows you to connect your workstation to your MetaFrame servers, regardless of the operating system they may be running. The client code is free to download from Citrix's Web site at:

<http://www.citrix.com/download/>

At the time of writing, the latest English version for AIX was Version 6.00.917. A version number of 6.x indicates that this is the new breed of clients with vastly enhanced features compared to the Version 3.x generation of ICA clients. Some of the Version 6.x features are:

- |                                |  |
|--------------------------------|--|
| <b>Increased color depths</b>  | The client now supports sessions with color depths of 16 and 24 bits per pixel.  |
| <b>Increased resolution</b>    | The client now supports sessions larger than 1280x1024. The theoretical maximum size is 32767x32767.   |
| <b>Seamless windows</b>        | Published applications may now be displayed in seamless window mode. This creates a separate client panel to display each application panel. These panels may be individually moved, resized, and iconified. Several published applications can share a session, conserving server resources and licenses. |
| <b>Speedscreen</b>             | Latency reduction. On slow connections, this feature gives rapid feedback for keyboard and mouse input.  |
| <b>Netscape plug-in module</b> | Allows an ICA session to be displayed as part of a Web page in a Netscape browser.   |

<b>SOCKS support</b>	The client can negotiate with a SOCKS server to allow a session to pass through a firewall.
<b>Secure ICA</b>	Provides strong encryption for ICA sessions.
<b>RTF clipboard support</b>	The client now supports the cutting and pasting of data in Microsoft Rich Text Format.

Installing the client is very straightforward once you have downloaded the code and unpacked it to a temporary directory on your system. Version 6.00.917 of the ICA Client does not support installation on AIX 5L, so we have to make a minimal change to the installation script for everything to work.

Make sure you are logged in as root and changed to the directory where you have placed the installation code for the ICA Client (in our case, the /tmp/icaInt directory).

The file we need to modify is ./ibm/hinst, so open this file with your favorite editor and search for the calc\_space\_available() function. The following screen highlights where you should add support for AIX 5L by inserting a "l5":

```

os_version=`uname -v`
case "$os_version" in
3)
    SPACE_AVAILABLE=`df ${inst_fs_dir} | awk '
        NR==2{avail=$3}
        END {print avail}'`
    ;;
4|5)
    SPACE_AVAILABLE=`df -k ${inst_fs_dir} | awk '
        NR==2{avail=$3}
        END {print avail}'`
    ;;
*)
    $ECHO_CMD $chkpace1
    $ECHO_CMD $chkpace2
    SPACE_AVAILABLE=0

```

Because the `df` command has not changed its output format between AIX 4.x and AIX 5L, we can safely add the "or 5" statement to the case evaluation. Save the file and start the installation by executing the `setupwfc` installation script.

An example of the initial installation dialog is shown in the following screen.

```
Select a setup option:

1. Install Citrix ICA Client 6.00
2. Remove Citrix ICA Client 6.00
3. Quit Citrix ICA Client 6.00 setup

Enter option number 1-3 [1]:1

Please enter the directory in which Citrix ICA Client is to be installed.
[default /usr/lib/ICAClient]
or type "quit" to abandon the installation: /usr/lib/ICAClient

You have chosen to install Citrix ICA Client 6.00 in /usr/lib/ICAClient.

Proceed with installation? [default n]:y
```

You will now be presented with the license agreement. Assuming you accept it, the installation continues as follows:

```
Continue with installation? [default n]:y
Installation proceeding...

Checking available disk space ...

        Disk space available 42440 K
        Disk space required 3970 K

Continuing ...
Creating directory /usr/lib/ICAClient
Core package...
6228 blocks
Setting file permissions...
Integrating with Netscape browser...
Integration complete.

Select a setup option:

1. Install Citrix ICA Client 6.00
2. Remove Citrix ICA Client 6.00
3. Quit Citrix ICA Client 6.00 setup

Enter option number 1-3 [1]: 3
Quitting Citrix ICA Client 6.00 setup.
```

If you do not have Netscape installed, you will be asked if you still want to add the plug-in. You probably do not want to add it, as installing Netscape at a later time will still require you to add the plug-in manually and it will be much easier to reinstall the ICA Client at that point.

Add the ICA Client installation directory to the path:

```
# export PATH=$PATH:/usr/lib/ICAClient
```

If you install the ICA Client in another directory, you will have to modify the above path and set the ICAROOT variable to the correct location.

### 5.6.3 MetaFrame for Windows 2000

MetaFrame for Windows 2000 Version 1.8a requires Terminal Services to be installed and configured for Application Mode operation. This in turn requires the presence of a Terminal Server Licensing server on your network.

#### 5.6.3.1 MetaFrame for Windows 2000 installation

Installing MetaFrame on a Windows 2000 server is a straightforward operation with very few options to consider. To start the installation, insert the CD and let it autostart or manually launch the <CD>:\I386\setup.exe file to start the installation. After accepting the license agreement, click **Next** > two times to get past the Welcome panel and the “Setting up MetaFrame” panel.

All files will then be copied to your system, and the configuration starts by allowing you to add license packs to the server. Enter your license information and click **Next** > to get to the Network ICA Connections panel shown in Figure 131 on page 222.

#### Note

All of the installation instructions refer to MetaFrame 1.8a for Windows 2000. The new flagship product from Citrix is MetaFrame XP for Windows 2000, which adds functionality and improves scalability. Unfortunately, this product was not available for testing at the time of writing.

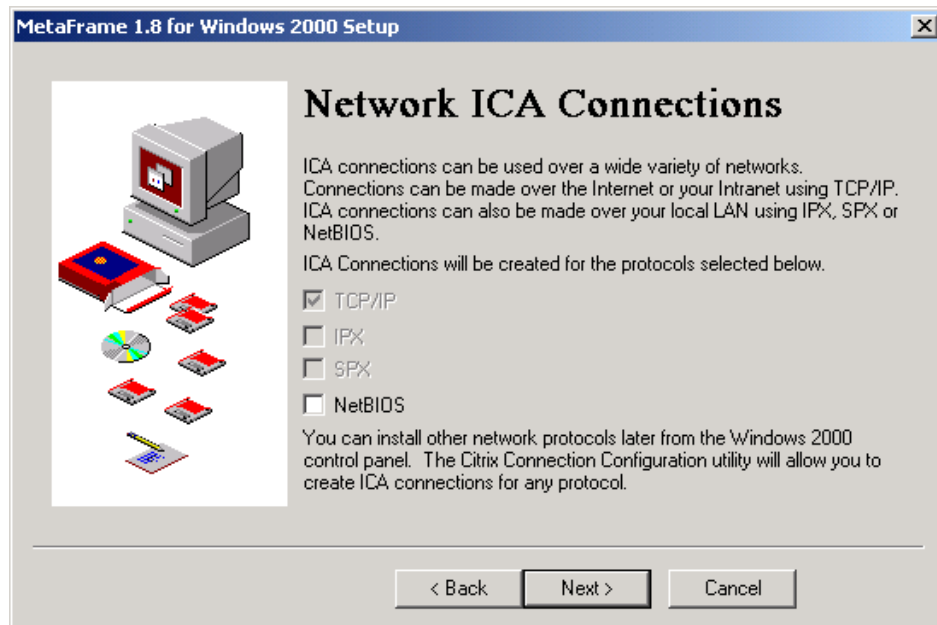


Figure 131. MetaFrame Win2K - Network ICA connections

Because TCP/IP is installed on the server, this protocol will be selected by default and greyed out. You can select all the protocols you want to support client connections with. However, a good idea is to start with only TCP/IP and add protocols as they become necessary.

Next, you can add and configure TAPI (Telephone API) modems if this functionality is needed for your environment. Click **Next >** to continue and continue to click **Next >**, leaving the Drive Mapping configuration as is, until you get to the last step of the installation, which is the System Reboot. When you click **Finish**, the machine will reboot. Make sure that you have closed all applications and that no users are active on your server.

After rebooting, you are ready to accept ICA connections without any further configuration.

### **Feature Release 1**

Feature Release 1 is an add-on to MetaFrame, adding a set of features to your MetaFrame server, including:

- **RC5 128-bit Encryption** - Feature Release 1 includes all of the functionality previously included in the 128-bit North American version of Citrix SecureICA Services.



- **NFuse 1.5 support** - An updated version of the Citrix XML Service, previously called Citrix NFuse Services, and installed as part of the NFuse for MetaFrame component.
- **Save ICA session starting position** - Version 6.0 of the ICA Client saves the position of ICA session panels between sessions. The panel for new connections is displayed in the same location where the previous connection was running.
- **Multi-monitor support** - Supports the multi-monitor features of Microsoft Windows 98 and Windows 2000 clients. It also supports the virtual desktop feature provided by some graphics cards for Windows 95 and Windows NT 4.0.
- **Panning and scaling** - Supports panning and scaling ICA session panels. If the ICA session is larger than the client computer's desktop, you can pan the ICA session panel around the full session desktop. Scaling allows you to view more of the ICA session at one time without panning by shrinking the perceived size of the ICA session.
- **Pass-through authentication** - This feature provides the ability to optionally pass the user's local desktop password to the MetaFrame server, eliminating the need for multiple system and application authentications.
- **TCP based ICA browsing** - Version 6.0 of the ICA Client can communicate with the updated Citrix XML Service to enumerate servers and published applications without using the UDP protocol.
- **ICA priority packet tagging** - Enables the prioritization of ICA virtual channels by third-party Quality of Service hardware.
- **Greater screen size** - Supports a maximum session size of 4524 by 3393 pixels. The previous maximum size was 1280 by 1024.
- **Greater color depth** - Supports high color (16 bit) and true color (24 bit) color depths for ICA sessions. The previous maximum color depth was 256 colors (8 bit).
- **Citrix SSL Relay** - The Citrix SSL Relay secures communications between NFuse-enabled Web servers and MetaFrame servers.
- **SpeedScreen Latency Reduction** - Version 6.0 of the ICA Client supports instant mouse click feedback and local text echo. These features greatly increase the perceived performance of ICA sessions over high latency connections. This feature is not available for the Japanese version of MetaFrame.

Feature Release 1 comes with Service Pack 2 for MetaFrame, which is installed automatically on your server to address around 20 known problems discovered since Service Pack 1 (SP1). SP2 contains all of the 30+ fixes from SP1.

At time of writing, there is one Post-SP2 Hotfix (available from the Citrix Web site) called ME182W001, which contains seven bug fixes.

### **Server configuration**

Configuration of MetaFrame is done using a set of different tools installed with the product. In this section, we assume that you have installed Feature Release 1. If you have not, some of the items could be missing or have a different appearance.

### **Activation Wizard**

This is a shortcut to <http://www.citrix.com/activate/login.htm>, where you activate your license codes.

### **Citrix Connection Configuration**

Citrix Connection Configuration is the equivalent of Microsoft Terminal Services Configuration, which still can be used to manage both RDP and ICA connection settings. Starting the application displays the panel shown in Figure 132.

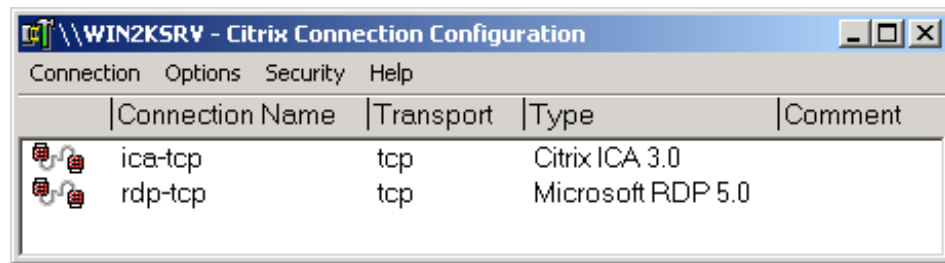


Figure 132. Citrix Connection Configuration

Because Terminal Services is installed on the machine, both RDP and ICA are valid protocols for connecting to the server. It is recommended that you minimize the use of RDP connections for ease of administration, but instead of disabling RDP entirely, change the permissions to allow only the administrator or your administrative group of choice. This could prove useful if you need to debug ICA settings and accidentally lock yourself out of the system.

**Note**

Do not mix up the Citrix ICA 3.0 connection type with the ICA 3.x or 6.x client.

By double-clicking on the ICA connection entry, or by right-clicking and selecting **Edit**, you will see the panel shown in Figure 133.

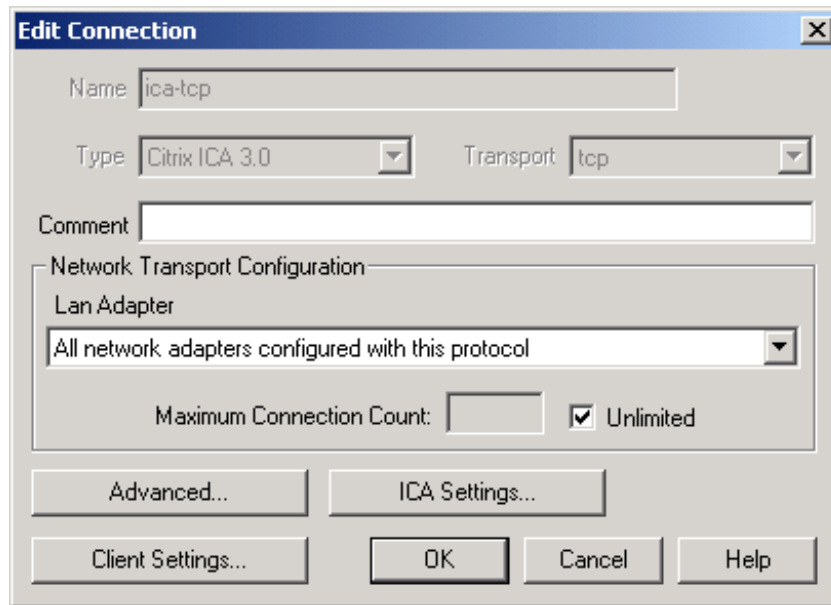


Figure 133. Edit Connection

The Advanced button will bring up a large panel with lots of settings, as seen in Figure 134 on page 226. Most settings are defined as “inherit user config,” indicating that you do not have a server preference. This allows the users to decide for themselves.

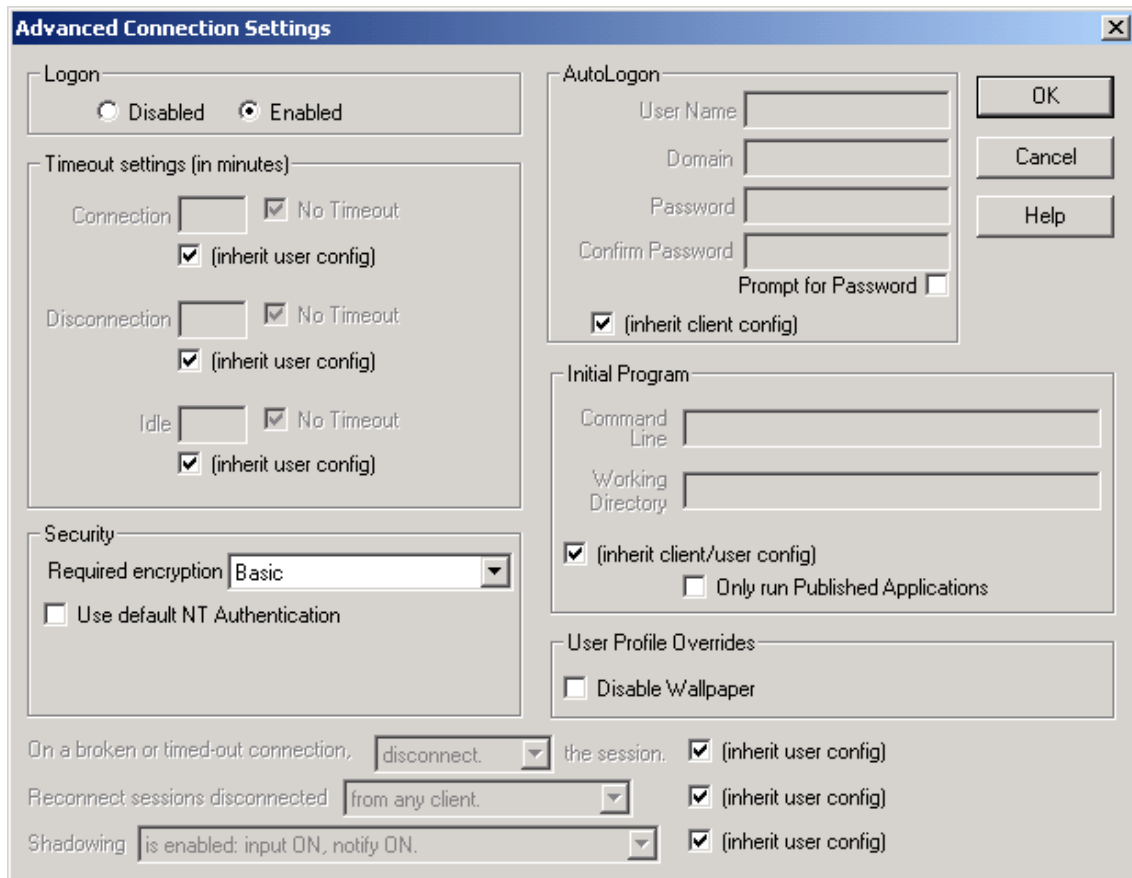


Figure 134. Advanced Connection Settings

Maybe the most important setting is the security options for various encryption levels. Your choices are:

- None
- Basic
- RC5 (128bit) login only
- RC5 (40bit)
- RC5 (56bit)
- RC5 (128bit)

The default is Basic, which merely scrambles the data and provides virtually no security at all. It is definitely recommended to change this to at least “RC5 (128bit) login only” if all your clients can comply.

From the Edit Connection Window, clicking the ICA Settings button allows you to configure the sound quality, depending on your available bandwidth.

The Client Settings button displays the panel shown in Figure 135, where you control the settings for various drive and port mappings.

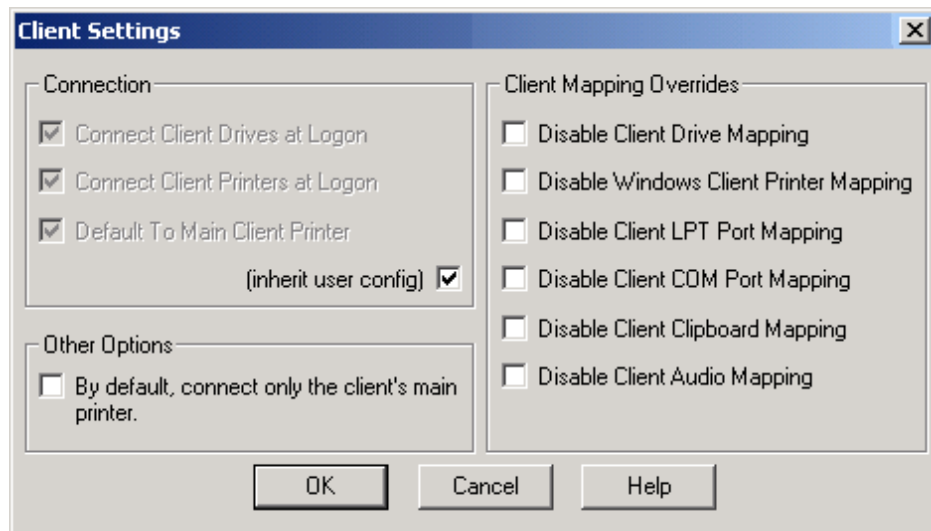


Figure 135. Client Settings

As mentioned earlier, all of these client connection functions are available using the Microsoft tool for Terminal Services Configuration.

### **Citrix Licensing**

Tool for adding, removing, and administering your Citrix licenses.

### **Citrix Server Administration**

The Server Administration tool allows you to monitor and terminate the connections to your servers, send messages to users, and control the browser functionality of the server, as seen in Figure 136 on page 228.

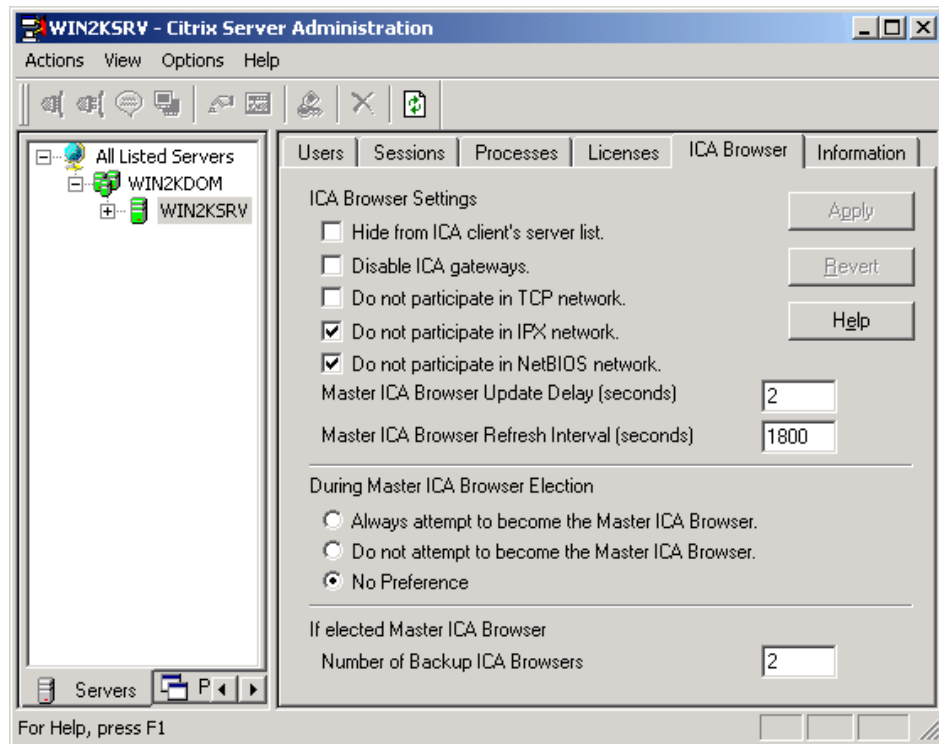


Figure 136. ICA browser configuration

Changes to Browser behavior should only be done if you know what you are doing. Assigning incorrect election criteria could generate unnecessary network load.

### ***Citrix SSL Relay Configuration Tool***

The Citrix SSL Relay Configuration Tool allows you to secure the communication between NFuse servers and MetaFrame servers.

### ***ICA Client Creator***

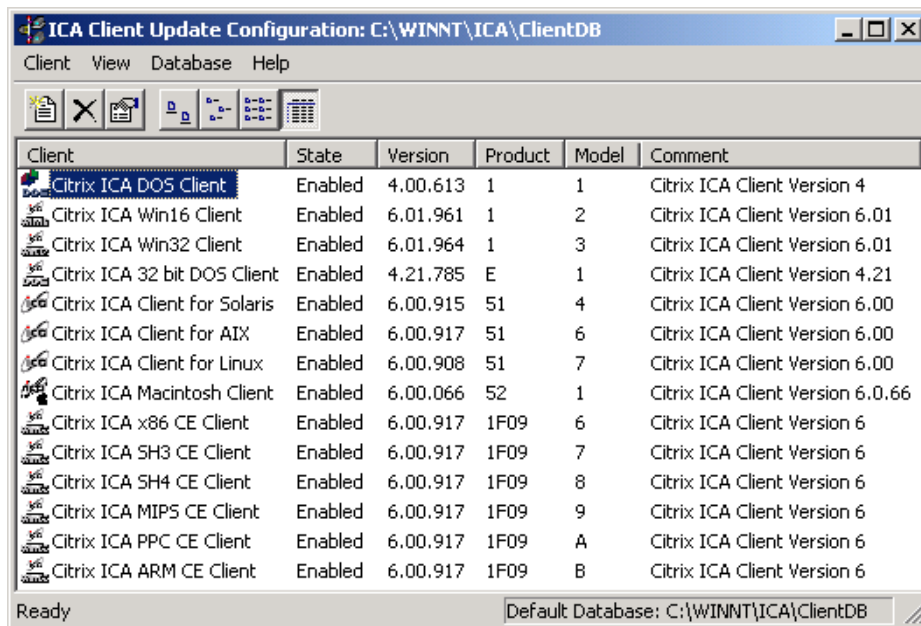
The Client Creator helps you create installation diskettes for ICA clients. This is useful when you are not able to connect to a server share for installation.

### ***ICA Client Printer Configuration***

This tool can only be run within an ICA session, and helps you control the way printers are mapped from your client through the ICA session to your server applications.

### **ICA Client Update Configuration**

The MetaFrame server has an ICA client database in which it stores the latest versions of the ICA clients for various operating systems. When a client connects to the server, the version of the ICA client is compared to the version in the database; if the database holds a more recent version, the client is automatically updated. A sample view of the ICA client database is shown in Figure 137.



The screenshot shows a window titled "ICA Client Update Configuration: C:\WINNT\ICA\ClientDB". The window has a menu bar with "Client", "View", "Database", and "Help". Below the menu bar is a toolbar with icons for file operations and database management. The main area contains a table with the following columns: Client, State, Version, Product, Model, and Comment. The table lists various Citrix ICA clients for different operating systems, all with a state of "Enabled".

Client	State	Version	Product	Model	Comment
Citrix ICA DOS Client	Enabled	4.00.613	1	1	Citrix ICA Client Version 4
Citrix ICA Win16 Client	Enabled	6.01.961	1	2	Citrix ICA Client Version 6.01
Citrix ICA Win32 Client	Enabled	6.01.964	1	3	Citrix ICA Client Version 6.01
Citrix ICA 32 bit DOS Client	Enabled	4.21.785	E	1	Citrix ICA Client Version 4.21
Citrix ICA Client for Solaris	Enabled	6.00.915	51	4	Citrix ICA Client Version 6.00
Citrix ICA Client for AIX	Enabled	6.00.917	51	6	Citrix ICA Client Version 6.00
Citrix ICA Client for Linux	Enabled	6.00.908	51	7	Citrix ICA Client Version 6.00
Citrix ICA Macintosh Client	Enabled	6.00.066	52	1	Citrix ICA Client Version 6.0.66
Citrix ICA x86 CE Client	Enabled	6.00.917	1F09	6	Citrix ICA Client Version 6
Citrix ICA SH3 CE Client	Enabled	6.00.917	1F09	7	Citrix ICA Client Version 6
Citrix ICA SH4 CE Client	Enabled	6.00.917	1F09	8	Citrix ICA Client Version 6
Citrix ICA MIPS CE Client	Enabled	6.00.917	1F09	9	Citrix ICA Client Version 6
Citrix ICA PPC CE Client	Enabled	6.00.917	1F09	A	Citrix ICA Client Version 6
Citrix ICA ARM CE Client	Enabled	6.00.917	1F09	B	Citrix ICA Client Version 6

Ready Default Database: C:\WINNT\ICA\ClientDB

Figure 137. ICA client database

### **Load Balancing Administration**

If you have multiple MetaFrame servers in the same 'farm,' use the Load Balancing feature to increase the availability and manageability of your applications.

### **Published Application Manager**

Publishing an application allows you to provide a very controlled environment to your users, compared to publishing a desktop. Publishing a desktop requires measures to lock down the environment, whereas publishing an application only gives the user access to that particular program.

The Published Application Manager gives you one place to add, delete, and configure applications for all your server farms.

### ***Shadow Taskbar***

The concept of shadowing is basically a remote control function for an ICA connection. As the whole concept of ICA is to move the GUI from server A to client B, replicating the screen to administrator C is as easy as it is convenient. The Shadow Taskbar adds a new taskbar to your desktop from which you easily can select a session to shadow.

### ***SpeedScreen Latency Reduction Manager***

SpeedScreen is a combination of technologies implemented in ICA that decreases bandwidth consumption by including local text echo and mouse click feedback. Together, these features enhance the user experience on a slow network. SpeedScreen settings can be configured on a per-application, per-server, and per-client basis.

### **5.6.3.2 ICA Client installation on Windows 2000**

Installing the ICA client on a Windows machine is a very straight-forward task, whether you start the installation using diskettes, mapping to an installation share on your network, or using a single file downloaded from the Citrix Web site.

The first few panels in the installation wizard are fairly basic and should not require any explanation. When you get to the ICA client name panel, shown in Figure 138 on page 231, you have to decide if you want to keep your computer name as the ICA client name, or if you need another naming standard. It is recommended that you keep the default name unless you are certain you need to change it.



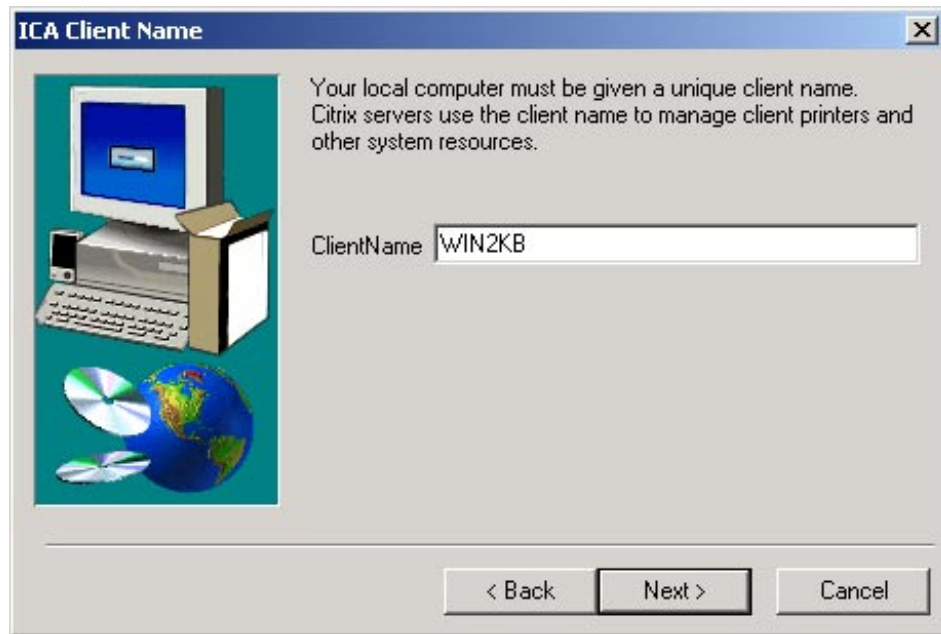


Figure 138. ICA Client name

After clicking **Next >** on the ICA Client Name question, the final panel for the installation lets you decide whether you want to integrate the authentication with the local user name and password. This feature works best if you are a member of the same domain as the MetaFrame servers or have your user credentials synchronized with the MetaFrame domain. If the user name and password you use when logging on to your machine is different from the one used in your ICA sessions, you will be queried for username and password anyway and will not benefit from the integration.

After the installation, you will need to reboot your client for all features to be enabled, but you could start using the client right away.

#### 5.6.4 Example: Running IE5 from an AIX session

As an example of how conveniently a published application can be used from any platform, we will use Internet Explorer 5.5 on a Windows 2000 server and run it from an AIX workstation.

No effort is done to lock down the Windows 2000 machine or support roaming profiles for IE settings and bookmarks.

We start by selecting the **Published Application Manager** from the **MetaFrame Tools** menu. When the application has scanned the network for applications, we select the **Application -> New** menu and the panel in Figure 139 is shown, asking you for the name of the application and an optional description. The name can be anything you like and does not have to correspond to the actual file name or application name.

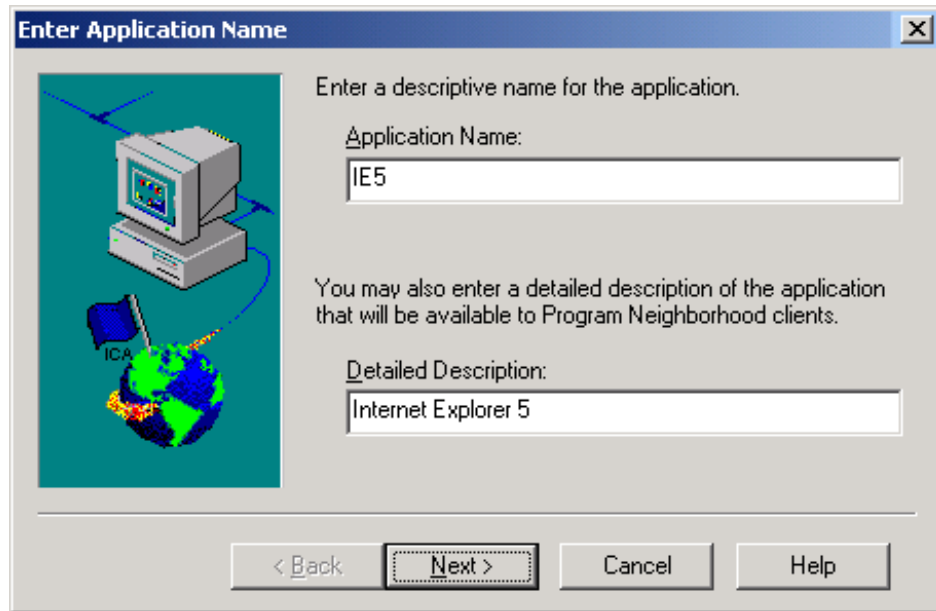


Figure 139. Enter Application Name

We enter an application name of "IE5," which is what will show up when we later broadcast the network for applications. Click **Next >** to continue.

The next panel asks you if this application should be published as an explicit or anonymous application. Select **Explicit** and the click **Next >**.

Next, we have to specify the application itself. Use the **Browse...** button and navigate your way to your executable file, as seen in Figure 140 on page 233. The working directory will be automatically filled in for you, but you are free to change it as you see fit. Click **Next >** to continue.

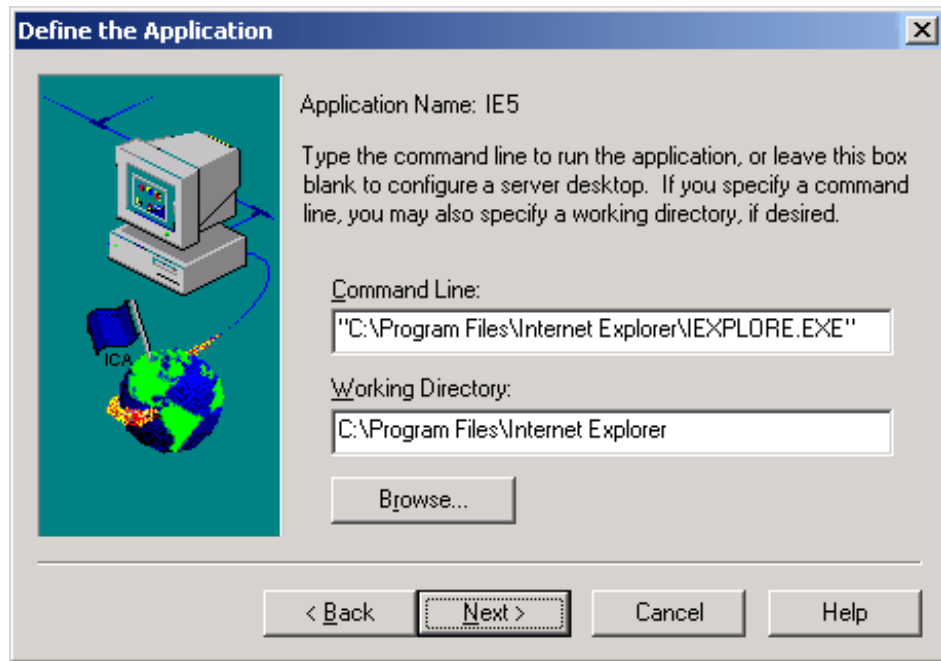


Figure 140. Define the Application

The 'Specify Window Properties' dialog allows you to hide the application title bar and maximize the application at startup. Because we will use this application in *Seamless Mode*, these settings will be ignored, so we can leave them at their default values.

Seamless Mode allow you to integrate your published applications into the program manager of the client operating system, whether this is X Window, CDE, or OS/2 Presentation Manager.

Click **Next >** to continue and **Next >** again to accept all the Program Neighborhood client settings. Unless you want to specify a minimum requirement for your application, all these settings will be controlled from the ICA client.

The Neighborhood Administration Features facilitates the distribution of new applications in your organization by proactively pushing the applications to the users desktops or Program Neighborhoods. We will not demonstrate this feature, so click **Next >** to continue.

If we have more than one Windows 2000 domain running Citrix MetaFrame, the next panel, seen in Figure 141, will give us the opportunity to specify the domain or server that will take care of the authentication for us.

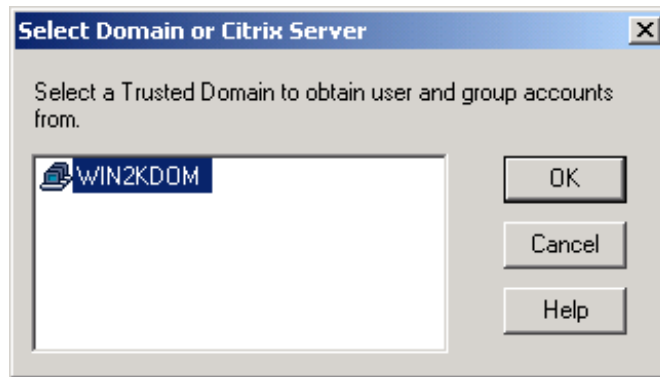


Figure 141. Select Domain or Citrix Server

In our case, the selection is easy because we only have one domain. Make your selection and click **OK**.

Now we determine what users or groups will have access to this application by selecting resources from the left pane and adding them to the right, as seen in Figure 142 on page 235. It is not recommended to explicitly grant access to individual users unless you are sure this is what you want. The reason is that if you have a lot of users and groups or a lot of applications published, it is much easier to add or remove a user from a group than to go through all applications and verify the presence or absence of a user entry.

In this example, we will allow all members of Domain Users to access our published Internet Explorer. Note that these rights do not affect what the user can do on the machine once an ICA session is established. This has to be controlled using policies and ACLs on the Windows 2000/MetaFrame server itself.

Click **Next >** to continue.

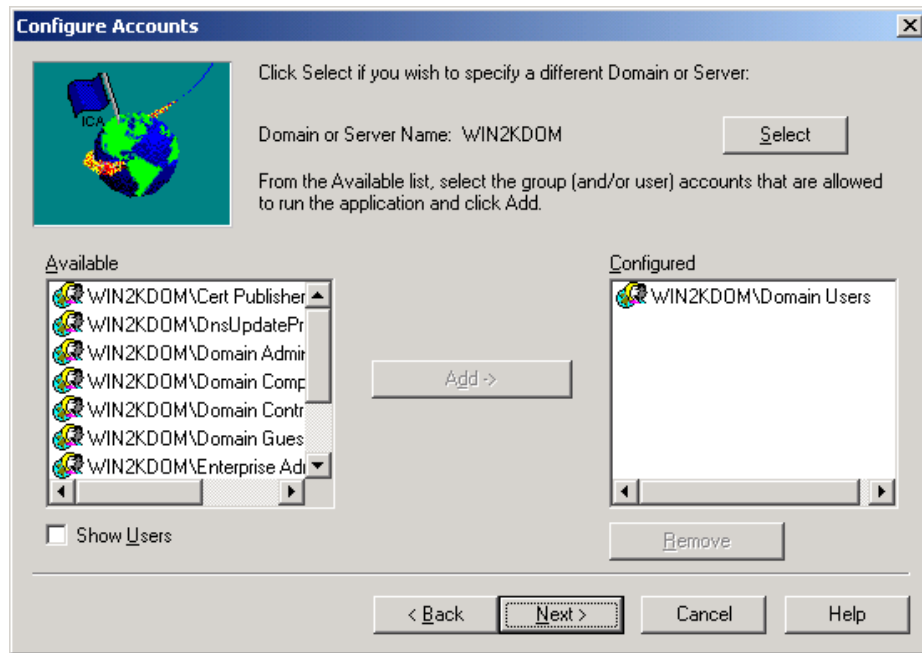


Figure 142. Configure Accounts

Next, you select the server(s) that will take part in offering the application to users. If you only have one server, you can simply click **Next >** to continue, but if your MetaFrame server is part of a server farm, you have to define which servers have this application installed and configured for users.

The last panel should confirm the success in creating your published application and allow you to either go back to make changes or click **Finish** to end the publishing wizard.

When you are returned to the Published Application Manager, your application should be present and enabled for use, as seen in Figure 143 on page 236.

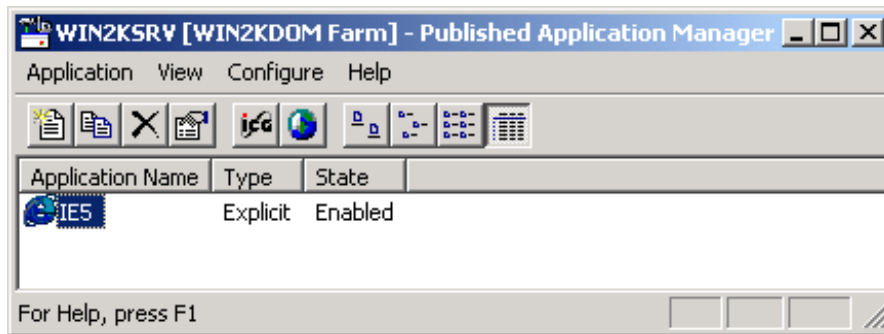


Figure 143. IE5 successfully published

We are now ready to move over to our AIX workstation for the final demonstration of published applications.

For a description on how to install the ICA client in AIX 5L, see Section 5.6.2.2, "ICA Client installation on AIX" on page 218.

Start the ICA client manager, either by clicking on it or by starting it from the command line with the `wfcmgr` command.

You should see the an ICA application manager as shown in Figure 144.

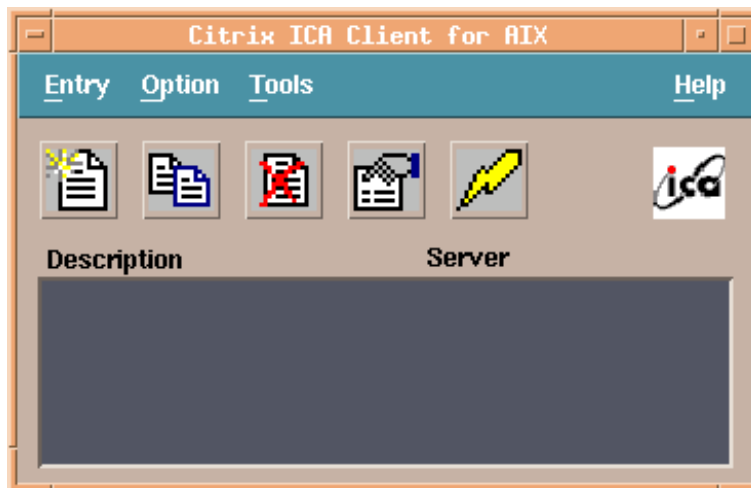


Figure 144. Empty AIX ICA client

Select the **Entry** -> **New** menu option, which should open the panel shown in Figure 145 on page 237.

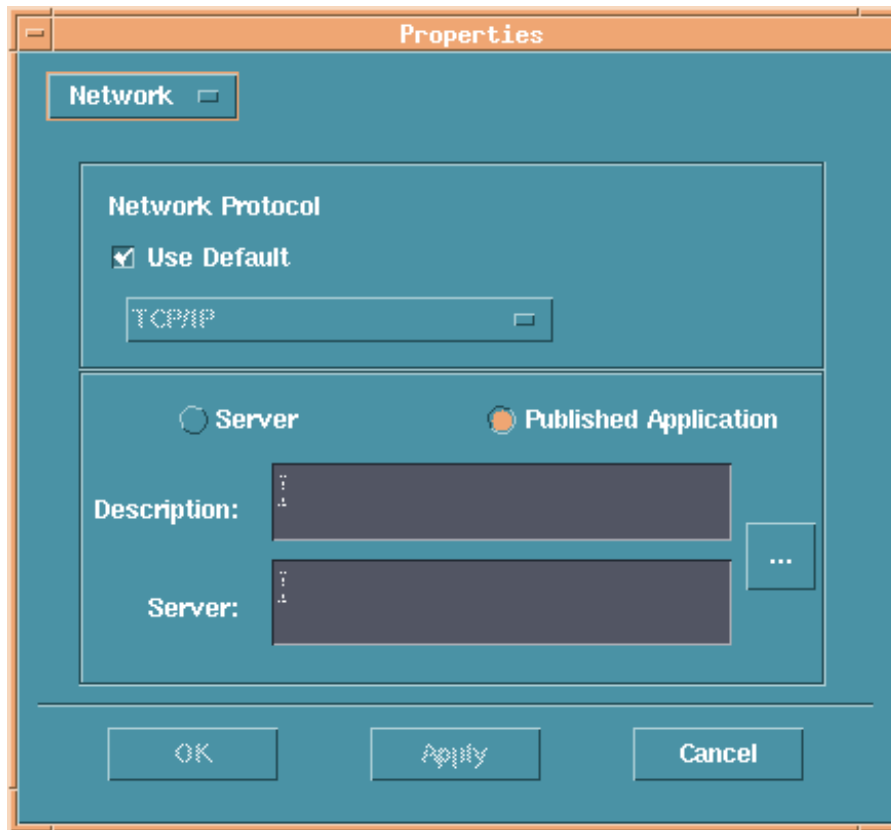


Figure 145. Network properties

Make sure you have selected **Published Application** and then click the ... button to search the network for available applications. Provided that your AIX machine is on the same subnet as your MetaFrame server, you should instantly be presented with a list of applications, as shown in Figure 146 on page 238.

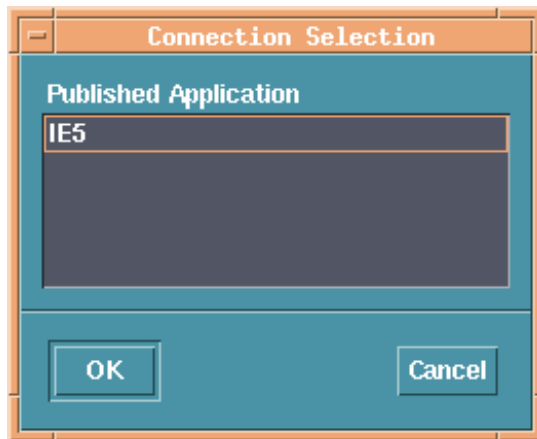


Figure 146. Connection Selection

Select your application and click **OK**, returning you to the panel in Figure 145 on page 237. In the upper left corner, you can see a button marked **Network**. Click this button and select **Window** from the menu that appears. This displays the panel shown in Figure 147 on page 239 containing all panel information for this application. Unless you have changed the default color settings of your ICA client, 256 colors will be the default value, and you will probably want to change this to a higher value because we will be using high color graphics in our browser. You also want to make sure you have checked the **Seamless Window** button, as this will give us a very smooth integration with our CDE desktop.



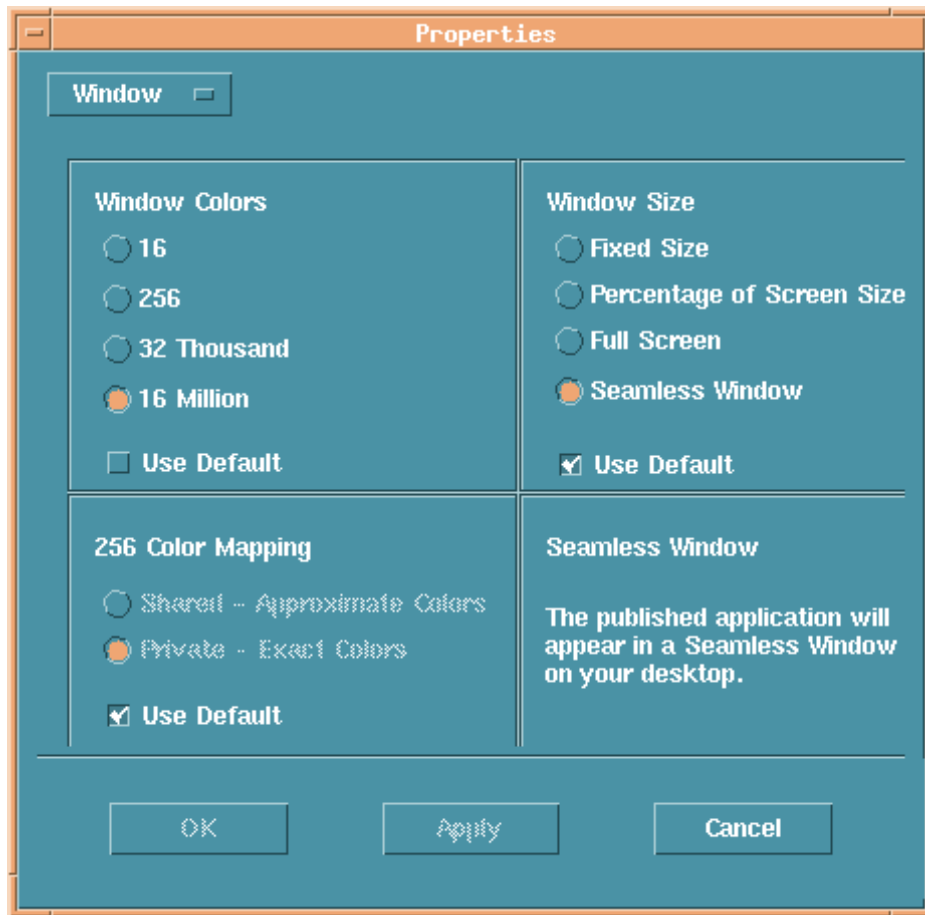


Figure 147. Window properties

If you prefer, you could fill out the login panel as well and when you are done, click **OK** to return to the Application Manager panel, shown in Figure 148 on page 240 (now containing our application).

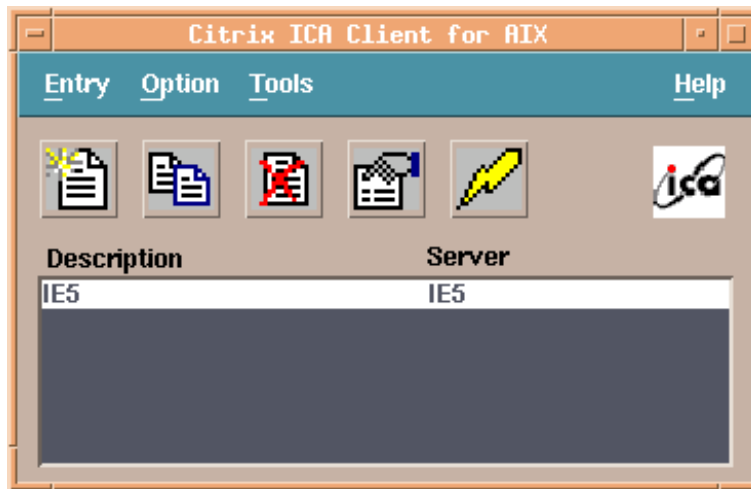


Figure 148. IE5 defined as an ICA application

Notice that the Server is indicated as IE5 as well. The reason for this is that we have not specified a specific server that we want to connect to, but rather an application we want to use. If we have multiple servers, all providing IE5 as a published application, the server with the least load will be the one servicing our request.

Clicking the Flash button or double-clicking on IE5 in the application list will start the application like any other CDE application as seen in Figure 149 on page 241. You are free to move, re-size, minimize, or close the application.

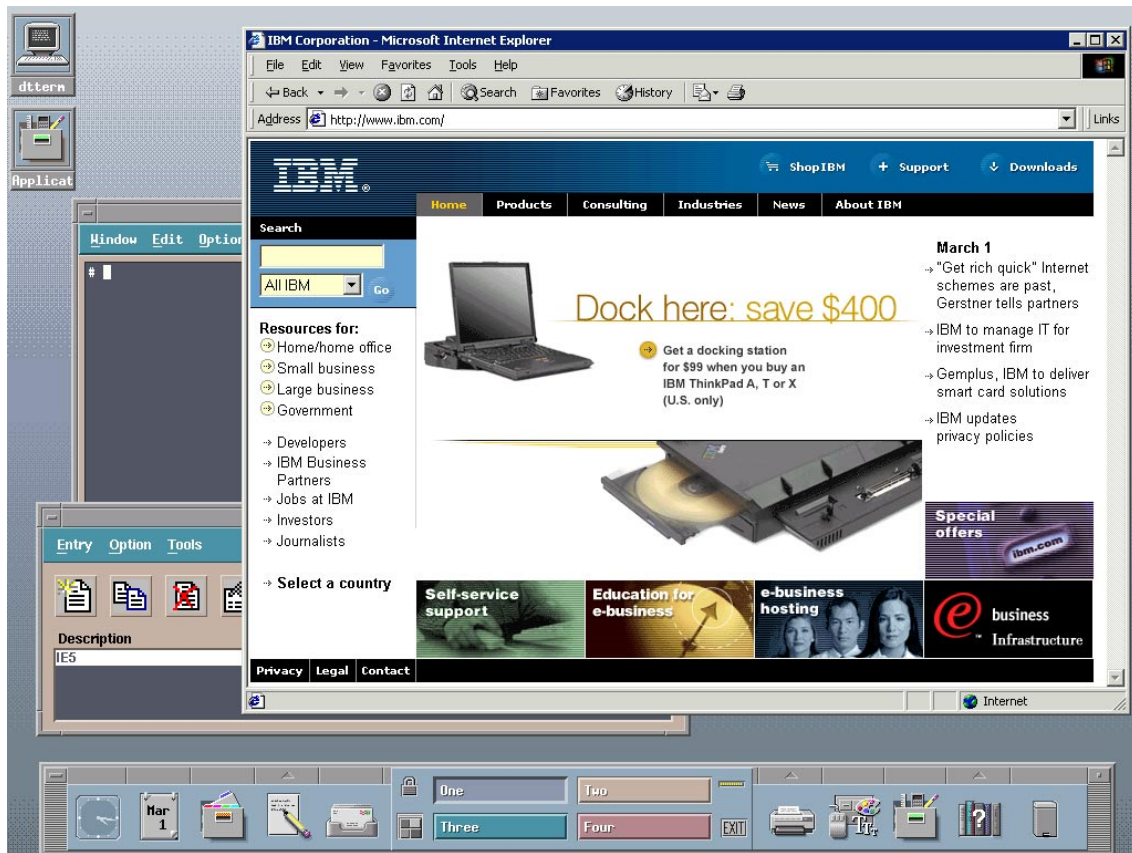


Figure 149. IE5 running seamless in CDE



## Appendix A. SFU UNIX utilities

Table 17 lists UNIX utilities included with SFU 2.0.

Table 17. SFU 2.0 UNIX utilities

Name	Function
basename	Prints the filename portion of a path name.
cat	Types a file or standard input to standard output device or specified file.
chmod	Changes permissions associated with a file or directory.
chown	Changes ownership of a file or directory.
cp	Copies files and directories.
cron	Schedules tasks.
crontab	Lists scheduled tasks and edits them.
cut	Cuts data at any point.
date	Writes date and time.
diff	Compares two files and displays line-by-line differences.
dirname	Prints base portion of path name (excluding the file name).
dos2unix	Converts text file from DOS to UNIX file format.
du	Prints the disk usage of file or directory.
egrep	Searches a file for a pattern using full regular expressions.
fgrep	Searches a file for a fixed character string.
find	Finds files in a hierarchy.
grep	Searches a file for a pattern.
head	Displays the first few lines of a file or standard input.
kill	Terminates or signals processes.
ln	Makes hard or symbolic links to files.
ls	Lists the contents of a directory.
mkdir	Makes directories.
more	Browses through files one screen at a time.
mv	Moves files or directories.

<b>Name</b>	<b>Function</b>
nice	Invokes a command with a specified scheduling priority.
od	Octal dump.
paste	Merges corresponding or subsequent lines of files.
perl	Perl engine.
printenv	Prints environment variables that are set.
printf	Writes formatted output.
ps	Lists processes or status.
pwd	Prints the current working directory.
rcmd	Runs a command remotely and returns information.
rcmdsvc	Service for rcmd.
renice	Reprioritizes a running process.
rm	Removes files/directory entries.
rmdir	Removes a directory entry.
rshsvc	Rsh service.
sdiff	Prints differences side-by-side.
sed	Stream editor.
sh	Korn shell.
sleep	Suspends execution for a specified interval.
sort	Sorts, merges, or sequences check text files.
split	Splits a file into pieces.
strings	Finds printable strings in an object or binary file.
su	Becomes another user (or administrator).
tail	Prints the last few lines of a file or standard output.
tee	Replicates to standard output.
top	Shows the top processes sorted by CPU usage.
touch	Changes a file's access and modification times.
tr	Translates characters in an input stream.

<b>Name</b>	<b>Function</b>
uname	Prints the name of the current system.
uniq	Reports or filters repeated lines in a file.
unix2dos	Converts a text file from UNIX to DOS file format.
vi	Visual Editor.
wait	Waits for a specified process to terminate.
wc	Word count.
which	Identifies the location of a given command.
xargs	Constructs argument lists.





## Appendix B. From 0 to NIS in 10 easy steps

In this appendix, we will describe how we set up NIS on AIX 5L to integrate user and group management with Windows 2000 using Services for UNIX Version 2.0.

This is in no way a complete guide to NIS, but instead a quick run-through of our configuration for those of you not familiar with NIS, but who would like to test the functionality of Microsoft Services for UNIX Version 2.0.

Services and functions might be added or deleted in a production environment, but this will produce a working environment for test and evaluation.

1. Starting with a basic install of AIX 5L, we add the following three components from the AIX 5L distribution:

```
# lslpp -L bos.net.nis*
bos.net.nis.client5.0.0.0Network Information Service
bos.net.nis.server5.0.0.0Network Information Service
bos.net.nisplus5.0.0.0Network Information Services Plus
```

2. Set the NIS domainname to nisdomain.com using the following commands:

```
# domainname nisdomain.com
# chypdom -I nisdomain.com.
```

Note the "." at the end of the domainname for the `chypdom` command, but not for the `domainname` command.

3. Stop and start the keyserver:

```
# stopsrc -s keyserv
# startsrv -s keyserv
```

4. Define the NIS admin group for the configuration script:

```
# NIS_GROUP=admin.nisdomain.com.
# export NIS_GROUP
```

Note the "." at the end of the groupname.

5. Add `/usr/lib/nis` to the PATH variable:

```
# PATH=$PATH:/usr/lib/nis
# export PATH
```

6. Create a root master server:

```
# nisserver -r -d nisdomain.com.
```

Again, note the "." at the end of the domainname.

7. Create a directory for NIS import files called /nis+files:

```
# mkdir /nis+files
```

8. Copy files from the /etc directory containing information that should be imported into NIS:

```
# cp /etc/group /nis+files
# cp /etc/hosts /nis+files
# cp /etc/passwd /nis+files
# cp /etc/aliases /nis+files
```

9. Populate the NIS database using the `nispopulate` command:

```
# nispopulate -F -p /nis+files -d nisdomain.com.
```

10. You should now have a fully functional NIS database that can be queried from the User Name Mapping Server in SFU.

## **Appendix C. Special notices**

This publication is intended to help system engineers, I/T architects, and consultants understand the various products that can be installed on the AIX operating system to better integrate with Windows 2000 systems. The information in this publication is not intended as the specification of any programming interfaces that are provided by AIX Fast Connect for Windows, Samba, FacetWin, MS Services for Unix, Exceed, PC-Xware, Reflection, or MetaFrame. See the publications section of the IBM Programming Announcement for AIX Fast Connect for Windows 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:

AFP	AIX
AIXwindows	AS/400
AT	Home Director
e (logo)® 	IBM ®
Netfinity	OS/2
Presentation Manager	Redbooks
RS/6000	Redbooks Logo 
SecureWay	SP
SP1	SP2

The following terms are trademarks of other companies:

Tivoli, Manage. Anything. Anywhere., The Power To Manage., Anything. Anywhere., TME, NetView, Cross-Site, Tivoli Ready, Tivoli Certified, Planet Tivoli, and Tivoli Enterprise are trademarks or registered trademarks of Tivoli Systems Inc., an IBM company, in the United States, other countries, or both. In Denmark, Tivoli is a trademark licensed from Kjøbenhavns Sommer - Tivoli A/S.

C-bus is a trademark of Corollary, Inc. in the United States and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States and/or other countries.

PC Direct is a trademark of Ziff Communications Company in the United States and/or other countries and is used by IBM Corporation under license.

ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel

Corporation in the United States and/or other countries.

UNIX is a registered trademark in the United States and other countries licensed exclusively through The Open Group.

SET, SET Secure Electronic Transaction, and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.

Other company, product, and service names may be trademarks or service marks of others.



---

## Appendix D. Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

---

### D.1 IBM Redbooks collections

Redbooks are also available on the following CD-ROMs. Click the CD-ROMs button at [ibm.com/redbooks](http://ibm.com/redbooks) for information about all the CD-ROMs offered, updates and formats.

CD-ROM Title	Collection Kit Number
IBM System/390 Redbooks Collection	SK2T-2177
IBM Networking Redbooks Collection	SK2T-6022
IBM Transaction Processing and Data Management Redbooks Collection	SK2T-8038
IBM Lotus Redbooks Collection	SK2T-8039
Tivoli Redbooks Collection	SK2T-8044
IBM AS/400 Redbooks Collection	SK2T-2849
IBM Netfinity Hardware and Software Redbooks Collection	SK2T-8046
IBM RS/6000 Redbooks Collection	SK2T-8043
IBM Application Development Redbooks Collection	SK2T-8037
IBM Enterprise Storage and Systems Management Solutions	SK3T-3694

---

### D.2 Referenced Web sites

These Web sites are also relevant as further information sources:

- [http://service.boulder.ibm.com/asd-bin/doc/en\\_us/winntc12/f-feat.htm](http://service.boulder.ibm.com/asd-bin/doc/en_us/winntc12/f-feat.htm)
- <http://www.samba.org>
- <http://www.samba.org/samba/ftp/samba-latest.tar.gz>
- <http://www-frec.bull.com/docs/download.htm>
- <ftp://ftp.samba.org/pub/samba/>
- <ftp://ftp.samba.org/pub/samba/samba-latest.tar.gz>
- <http://cvshome.org/>
- <http://www.samba.org/samba/docs>
- <http://www.samba.org/samba/support>
- <http://www.facetcorp.com/>
- <http://www.microsoft.com/downloads/search.asp>
- <http://www.ActiveState.com/>

- <http://www.ActiveState.com/ActivePerl/docs/faq/ActivePerlfaq.html>
- <http://msdn.microsoft.com/library/default.asp>
- <http://www.microsoft.com/hwdev/WMI/>
- <http://www2.hcl.com/html/forms/nc/exceed/request.html>
- <http://www.ncd.com/>
- <http://www.ncd.com/products/software/pcxware/pcxeval.html>
- [http://www.wrq.com/products/reflection/pc\\_unix/](http://www.wrq.com/products/reflection/pc_unix/)
- <http://www.citrix.com/activate/login.htm>
- <http://www.citrix.com/download/>
- [http://www.facetcorp.com/fw\\_download.html](http://www.facetcorp.com/fw_download.html)



## 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](http://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:

	<b>e-mail address</b>
In United States or Canada	pubscan@us.ibm.com
Outside North America	Contact information is in the "How to Order" section at this site: <a href="http://www.elink.ibm.com/pbl/pbl">http://www.elink.ibm.com/pbl/pbl</a>

- **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: <a href="http://www.elink.ibm.com/pbl/pbl">http://www.elink.ibm.com/pbl/pbl</a>

- **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: <a href="http://www.elink.ibm.com/pbl/pbl">http://www.elink.ibm.com/pbl/pbl</a>

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.



---

## Abbreviations and acronyms

<b>ACCON</b>	AIX Connection	<b>DMTF</b>	Distributed Management Task Force
<b>AFS</b>	Andrew File System		
<b>AIX</b>	Advanced Interactive eXecutive	<b>DNS</b>	Domain Name Service
<b>ANSI</b>	American National Standards Institute	<b>DOS</b>	Disk Operating System
<b>API</b>	Application Programming Interface	<b>FAT</b>	File Allocation Table
<b>ATM</b>	Asynchronous Transfer Mode	<b>FDDI</b>	Fiber Distributed Data Interface
<b>BDC</b>	Backup Domain Controller	<b>HACMP</b>	High Availability Cluster MultiProcessor
<b>CDE</b>	Common Desktop Environment	<b>HTML</b>	Hypertext Markup Language
<b>CIFS</b>	Common Internet File System	<b>iFOR/LS</b>	Information for Operation Retrieval/License System
<b>CIM</b>	Common Information Model	<b>IBM</b>	International Business Machines Corporation
<b>CN</b>	Common Names	<b>ICA</b>	Independent Computing Architecture
<b>CPU</b>	Central Processing Unit	<b>IETF</b>	Internet Engineering Task Force
<b>CSR</b>	Customer Service Request	<b>IPF</b>	Install Package Facility
<b>CVS</b>	Concurrent Version System	<b>IPX</b>	Internetwork Packet eXchange
<b>DAP</b>	Directory Access Protocol	<b>ITSO</b>	International Technical Support Organization
<b>DC</b>	Domain Controller	<b>JFS-ACL</b>	Journalled File System - Access Control List
<b>DCE/DFS</b>	Distributed Computer Environment/ Distributed File System	<b>LAN</b>	Local Area Network
<b>DECNet</b>	Digital Equipment Corporation Networking Protocol	<b>LANA</b>	Local Area Network Adapter
<b>DLPI</b>	Data Link Provider Interface	<b>LDAP</b>	Lightweight Directory Access Protocol
<b>DMB</b>	Domain Master Browser	<b>LMB</b>	Local Master Browser
		<b>LPP</b>	Licensed Program Products

<b>LPR</b>	Line Printer	<b>SAM</b>	Security Accounts Manager
<b>MB</b>	Megabyte	<b>SAP</b>	Service Advertising Protocol
<b>Mb</b>	Megabit	<b>SAPD</b>	SAP daemon
<b>MMC</b>	Microsoft Management Console	<b>SFU</b>	Services for Unix
<b>MSI</b>	Microsoft Installer	<b>SMB</b>	Server Message Block
<b>NBNS</b>	NetBios Name Server	<b>SMP</b>	Symmetric Multiprocessor
<b>NCP</b>	Network Core Protocol	<b>SNMP</b>	Simple Network Management Protocol
<b>NFS</b>	Network File System	<b>SP</b>	Scalable POWERParallel
<b>NIS</b>	Network Information System	<b>SPX</b>	Sequenced Packet eXchange
<b>NTFS</b>	NT File System	<b>SWAT</b>	Samba Web Administration Tool
<b>NetBEUI</b>	NetBIOS Extended User Interface	<b>TCP/IP</b>	Transmission Control Protocol/Internet Protocol
<b>NetBIOS</b>	Network Basic Input/Output System	<b>XDR</b>	eXternal Data Representation
<b>OEM</b>	Original Equipment Manufacturer	<b>VMS</b>	Virtual Memory System
<b>ONC RPC</b>	Open Network Computing Remote Procedure Call	<b>WINS</b>	Windows Internet Name Service
<b>Oplock</b>	Opportunistic locking	<b>WMI</b>	Windows Management Instrumentation
<b>PC</b>	Personal Computer	<b>XDM</b>	X Window Display Manager
<b>PDC</b>	Primary Domain Controller	<b>XDMCP</b>	X Windows Display Manager Control Protocol
<b>PPA</b>	Physical Point of Attachment		
<b>RAM</b>	Random Access Memory		
<b>RCS</b>	Revision Control System		
<b>RFC</b>	Request For Comments		
<b>RIP</b>	Routing Information Protocol		
<b>RS/6000 SP</b>	IBM RS/6000 Scalable POWERParallel Systems		

## Index

### Symbols

/etc/profile 213

### Numerics

2EE 51

2EF 51

2F0 51

2F1 51

2F2 51

2F3 51

2F4 51

2F5 51

### A

Access Control Lists (ACLs) 168

Accessing 114

ACLs 168

ActiveX 209

Advanced Server for UNIX 32

AIX

dtlogin 183, 189

export X Windows 202

XDM 183

XDMCP 183

xterm 201, 202

AIX Connections 32

AIX Fast Connect 3

Accessing resources 46

cifsClient 34

cifsConfig 35

cifsLog 35

cifsPasswd 35

cifsPrintServer 34

cifsPrintServerDCE 35

cifsServer 34

cifsServerAdv 34

cifsServerAdvDemo 34

cifsTrace 35

cifsUserProc 34

Configuration 35

Limitations 55

Locating the server 44

Logs 52

Migrating from AIX Connections 53

net 34

parameters 35

Performance 54

problem determination 49

rc.cifs 34

server administration 40

sm\_smb.cat 35

Starting and stopping 37

User Administration 39

ANSI 171

ASCII 171

authentication

secure 96

### B

basename 243

browsing 58, 102

### C

cache\_searches 54

cat 243

CDE 183, 191, 207

export CDE 204

chmod 243

chown 243

Citrix MetaFrame 207

bandwidth 208

ICA 207

ICA clients 209

ICA concept 207

protocol stream 208

SecureICA 210

Citrix MetaFrame for AIX 210

\$MANPATH 213

\$PATH 213

ctxadm 210

ctxlicense 214

ctxshutdown 215

ctxsrvr 210

Feature Release 1 214

installation 210

man pages 213

Client for NFS

Default LAN 156

Favorite LAN 156

mount 151, 153

net use 151

- NFS Network 156
- NFSAdmin 154
- showmount 154
- UMASK 162
- umount 153
- command
  - smbclient 60, 75
  - smbtar 86, 89
  - testparm 74
- Common Desktop Environment
  - X Windows 183
- Common Internet File System (CIFS) 56
- Concurrent 59
- Concurrent Version System (CVS) 59
- cp 243
- cron 243
- CronSvc 131
- crontab 243
- cut 243

## D

- Datagram service 58
- date 243
- DCE 54
- DECNet 57
- DFS 54
- DHCP 43
- diff 243
- dirname 243
- DMTF 181
- Domain
  - authentication 96
- Domain Master Browser (DMB) 101
- Domain Name System (DNS) 57
- Domain security level 98
- Domain-level security 91
- DOS 108
- DOS application 86
- dos2unix 243
- du 243

## E

- egrep 243
- EnablePlainTextPassword 95
- encryption 92
- Entire Network 45
- Exceed 5, 183
  - CDE 186

- functionality 200
- installation 184
- setup 187
- Xconfig 188

## F

- FacetWin 3, 105
  - Agent Control Panel 118
  - commands 123
  - E-Mail Server 106
  - File and Print services 106
  - Installing 111
  - Modem Server 106
  - PC Backup/Restore 106
  - Remote Computing 106
- fct\_encrypt 110
- fctpasswd 110
- Feature Release 1 214
- fgrep 243
- find 243
- Find computer 44
- FTP 2, 7, 10
- FTP server service 7

## G

- Gateway for NFS 136
  - gwconfig 165
- GID 163
- global parameter
  - password server 96
  - security 96
  - username map 100
- grep 243

## H

- head 243
- HKEY\_LOCAL\_MACHINE 95
- Hummingbird 183
  - Exceed 183

## I

- ICA 207
- ICA clients 209
- installation
  - Exceed 184
  - PC-Xware 192
- Internet Information Services 7, 8

IPX 57, 207

## J

Java 209

JFS-ACLs 30

## K

kill 243

## L

LAN 207

LANMAN 110

LC\_MESSAGES 55

Linux 209

LMHOSTS 102

ln 243

Local Master Browsers (LMBs) 101

locale 55

lpd 16

lpr 16

LPR Port 20

ls 243

## M

Map Network Drive 47

Mapsvc 131

MetaFrame 5, 207

MetaFrame for Windows 2000 installation 221

Microsoft Services for UNIX 127

ActivePerl 128, 129, 178

CIM 181

Client for NFS 127, 129, 151

Command line installation 130

Common Information Model 181

components 127

CRON Service 128

File system components 151

Gateway for NFS 127, 129, 164

GUI installation 133

GUI un-installation and modification 136

Installation and customization 130

Korn shell 129, 178

Microsoft Management Console 179

MMC 129, 179

NIS to AD Migration Wizard 130, 150

Password Synchronization 127, 130, 141

Remote Shell Service 128

Server for NFS 127, 129, 168

Server for NFS Authentication 128

Server for NIS 127, 129, 149

Server for PCNFS 127, 129, 170

sfumgmt.msc 180

System Requirements 127

Telnet Client 128, 129, 176

Telnet components 170

Telnet Server 128, 129, 171

UNIX Shell and Utilities 128

UNIX utilities 129, 178

User and Security components 137

User Name Mapping 127, 130

User name mapping server 137

Windows Management Instrumentation 181

WMI 129, 181

mkdir 243

MMC 138

more 243

MSI 133

mv 243

My Network Places 44, 80

## N

Name service 58

NBNS 31

net 36

net statistics 49

net use 153

net view 45, 82

NetBEUI 207

NetBIOS 57, 82

NetBIOS Extended User Interface (NetBEUI) 57

NetBIOS name 101

NetBIOS over TCP/IP 56, 57

NetBios over TCP/IP 56

NetBIOS/ix for AIX 32

Network Basic Input/Output System (NetBIOS) 29, 57

Network Computing Devices 191

NFS 4, 54, 157, 163

NFSClient 131

NFSGateway 131

NFSServer 130

NFSServerAuth 130

nice 244

NIS 131

nmbd 61

NT Domain 55  
NT Lan Manager (NTLM) 28  
NTLM 171

## O

od 244  
oplocks 58

## P

Passthrough 52  
PasswdSync 131  
password 96  
    encrypted 92  
    unencrypted 93  
Password Synchronization 136  
    PasswordPropAllow 148  
    PasswordPropDeny 148  
PasswordPropAllow 148  
PasswordPropDeny 148  
paste 244  
PCNFS 138  
Pcnfsd 131  
PC-Xware 5, 191  
    download 192  
    functionality 202  
    installation 192  
Perl 129, 131  
perl 244  
ping 49  
POP3 106  
port 61  
PPP 108, 109  
printenv 244  
Printers 19, 67  
printf 244  
ps 244  
pwd 244

## Q

quota 55

## R

RC5 226  
rcmd 244  
rcmdsvc 244  
RDP 224  
Reflection 5, 198

renice 244  
Revision Control System (RCS) 59  
RHOST 110  
rm 244  
rmdir 244  
RshSvc 131  
rshsvc 244

## S

Samba 3, 32  
    back up a client 86  
    configuration file 72  
    daemons 61  
    Global parameters 73  
    Home 64, 65  
    Locating the server 80  
    parameters 66  
    security modes 91  
    Share parameters 73  
    Shares 66  
    Status 69  
sdiff 244  
Search Caching 54  
Search for Computers 45  
Search Now 45  
SecureICA 210  
Security 91  
sed 244  
send\_file\_api 55  
SendFile API 55  
Server for NFS  
    File locking 169  
    Logging 169  
    Network Lock Manager 169  
    NFS Version 2 168  
    NFS Version 3 168  
    NLM 169  
    ONC RPC 168  
    XDR 168  
Server for NIS 136  
Server for PCNFS 170  
Server Message Block (SMB) 29, 56, 58, 151  
Server-level security 91  
Services for UNIX 4  
Session service 58  
sh 244  
sh\_searchecache 54  
sh\_sendfile 55



share 73  
sleep 244  
SMB 3, 29, 57  
smb.conf 60, 75  
smbclient 60, 74, 75, 88  
smbd 61, 99  
smbpasswd 93  
smbtar 89  
SMIT 30  
sort 244  
split 244  
SSL 223  
sso.conf 142  
    CASE\_IGNORE\_NAME 144  
    ENCRYPT\_KEY 142  
    FILE\_PATH 143  
    NIS\_UPDATE\_PATH 144  
    PORT\_NUMBER 143  
    SYNC\_DELAY 144  
    SYNC\_HOSTS 143  
    SYNC\_RETRIES 144  
    SYNC\_USERS 143  
    TEMP\_FILE\_PATH 143  
    USE\_NIS 143  
    USE\_SHADOW 143  
ssod 142, 144  
strings 244  
su 244  
SWAT 60, 61, 62

## T

tail 244  
TCP/IP  
    export X Windows 183  
tee 244  
Telnet client  
    ANSI 177  
    VT-100 177  
    VT-52 177  
    VTNT 177  
Telnet server  
    active sessions 174  
    authentication 171  
    Default Domain Name 173  
    GUI configuration 171  
    logging 171  
    tnadmin 175  
TelnetClient 131

TelnetServer 131  
terminal emulation 4, 106, 183  
testparm 74  
top 244  
TotalNet Advanced Server for AIX 32  
touch 244  
tr 244  
Trace 51  
Troubleshooting 103

## U

UID 163  
ulimit 55  
umount 152  
uname 245  
Unicode 55  
uniq 245  
unix2dos 245  
UnixUtilities 131  
User Name Mapping Server 248

## V

vi 245  
virtual directory 11  
VT-100 171  
VT-52 171  
VTNT 171

## W

wait 245  
WAN 207  
wc 245  
Web-based System Manager 30  
which 245  
Windows 2000 76  
Windows for Workgroups 92, 95  
Windows Internet Name Service (WINS) 57  
WINS 58, 79, 100, 101  
WMI 129  
workgroup 77

## X

X Windows 191  
    X Display Manager 183  
xargs 245  
Xconfig  
    communication 200

- usage 188
- XDM setup 188
- XDM 183, 198
  - export X Windows 204
  - interoperability 200
  - query 196
- XDMCP 183, 198, 200
  - broadcast 191
  - XDMCP-query 188

## 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](http://ibm.com/redbooks)
- Fax this form to: USA International Access Code + 1 845 432 8264
- Send your comments in an Internet note to [redbook@us.ibm.com](mailto:redbook@us.ibm.com)

<b>Document Number</b>	SG24-6225-00
<b>Redbook Title</b>	AIX 5L and Windows 2000: Solutions for Interoperability
<b>Review</b>	        
<b>What other subjects would you like to see IBM Redbooks address?</b>	   
<b>Please rate your overall satisfaction:</b>	<input type="radio"/> Very Good <input type="radio"/> Good <input type="radio"/> Average <input type="radio"/> Poor
<b>Please identify yourself as belonging to one of the following groups:</b>	<input type="radio"/> Customer <input type="radio"/> Business Partner <input type="radio"/> Solution Developer <input type="radio"/> IBM, Lotus or Tivoli Employee <input type="radio"/> None of the above
<b>Your email address:</b> 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.	<input type="checkbox"/> Please do not use the information collected here for future marketing or promotional contacts or other communications beyond the scope of this transaction.
<b>Questions about IBM's privacy policy?</b>	The following link explains how we protect your personal information. <a href="http://ibm.com/privacy/yourprivacy/">ibm.com/privacy/yourprivacy/</a>





## AIX 5L and Windows 2000: Solutions for Interoperability







**Redbooks**

# AIX 5L and Windows 2000: Solutions for Interoperability

## **Sharing files and printers between AIX 5L and Windows 2000 systems**

This redbook is intended to help you understand how to integrate and optimize your AIX systems into Windows 2000 environments and share AIX resources with your Windows 2000 machines. We have focused our descriptions on the key areas of file and printer sharing.

## **Learn interoperable networking solutions**

This redbook will discuss the various connectivity solutions available for AIX 5L to interoperate with Windows 2000 machines, including AIX Fast Connect, Samba, FacetWin, Services for UNIX, Exceed, PC-Xware, Reflection, and MetaFrame.

## **Fully integrate and optimize Windows with your AIX environment**

Each chapter focuses on these solutions to help you decide which one is most appropriate for your specific needs. The second part of each chapter is a step-by-step approach to the installation, configuration, and customization of these 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](http://ibm.com/redbooks)

SG24-6225-00

ISBN 0738422118